

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

July/August 2013

© 2013 The Metropolitan Corporate Counsel, Inc.

Volume 21, No. 7

Data Collection In A Social Media World

The Editor interviews Daniel E. Roffman, FTI Consulting, Inc. Mr. Roffman is a Managing Director in the FTI Technology segment and is based in Chicago.

Editor: Tell us about your background and current role at FTI Technology.

Roffman: I've been with FTI for over seven years. Prior to that, I worked at the Department of Justice's child exploitation and obscenity section doing computer forensics. This work involved complex investigations relating to various forms of cybercrime, which operates very quickly, and I've worked on similarly time-sensitive projects in the e-discovery arena since coming to FTI.

Briefly, FTI uses computer forensics to collect data from myriad sources, including from mobile devices like iPhones, iPads, Android devices and BlackBerries; from laptops, desktops and servers; and from various web sources, such as social media, Dropbox and Google Drive.

Editor: What types of social media use cases are you seeing in corporations today?

Roffman: We are seeing two main types. The first involves more traditional investigation, usually limited to the actions of one or two people and concerned with answering the question "did this happen?" In terms of social media, this might require knowing if someone tweeted "X" message to "Y" person(s) at "Z" time, and the form of collection for discovery purposes may be as simple as printing out the social media page.

The second type involves broad-based employee communications, both inside and outside the company's walls. Employees might be instant messaging each other over Google Talk or communicating via email accounts on social media websites. In these cases, collection involves a much

wider set of custodians; it requires access to laptops and desktops, to the company's email server and, increasingly, to the web and sites like Facebook, Twitter or LinkedIn. With so much information available for discovery purposes, it's important to be able to filter out what's relevant before engaging attorneys for the review and production phases.



**Daniel E.
Roffman**

Editor: What are some of the top challenges you face with social media sites? With legal teams regularly facing discovery issues relating to over-preservation and over-collection, how do you keep projects focused on relevant data?

Roffman: Security features that users enable pose a challenge when accessing sources outside the company's direct control. The information that social media users choose to share publicly is not the full corpus of data in their accounts as it does not include private messages between users. So, depending on the case, we will determine the best collection methods, which might include obtaining a user's credentials and logging into their account or, perhaps, determining that the case can be handled based only on publicly available information.

Social media information presents special challenges because it is not in the same context as computer files. By imaging a computer, for example, we can very quickly filter out system files and focus, for instance, on Word, PowerPoint or Excel documents plus emails, and then apply keyword searches to reduce the population that goes on to the review stage. With social media, however, there's no defined document type. It's a web page that is constantly changing, so what you

collect today may look very different tomorrow.

In terms of collection methods, I already mentioned the simple option of printing out a PDF snapshot of someone's social media page; however, this might include a lot of irrelevant personal communication that will require an attorney's time to redact and cause the project to be less focused. When possible, we employ a technique that collects each individual item on a social media profile as a separate document. Then we can apply keyword searches, just as we do with traditional computer files, to produce a succinct collection of responsive documents for the attorneys to review. Companies often overlook the collection process – perhaps because it can be outsourced to an FTI Consulting – without considering the important downstream implications at the review stage.

Editor: Would you say this is a dynamic environment?

Roffman: Absolutely. Social media is changing the way that we do e-discovery and continuously blurring the lines between methods of interaction, such as instant messaging (IM) versus email or video chat. On Facebook, for example, you can IM someone who may or may not be online, so while it may appear to be "instant," it's actually treated more like an email.

We are very accustomed to e-discovery that involves documents and emails, but what happens when that email is now a video chat? All of our existing capabilities – such as collecting data, running keyword searches and exporting to third parties at the production phase – will need to be adapted dynamically and in line with constantly changing technology in the social media space.

One final point has to do with strategy for corporate clients and the attorneys who counsel them. If companies don't stay on top of the social media collection curve,

Please email the interviewee at dan.roffman@fticonsulting.com with questions about this interview.

then they might someday find themselves at a real disadvantage in facing an adversary that has kept current. Attorneys inside and outside the company have to know what's in their clients' social media pages, and FTI Technology can help with this.

Editor: How do the challenges of preservation and collection within social media carry over to the review process?

Roffman: We have already discussed the broad idea of collecting information in a manner that allows us take subsequent action aimed at limiting the attorney review process. Our approach is very granular: down to individual posts and tweets, where and when they were posted, and the number of "likes" or other responses. Preserving this metadata allows us to choose the most effective method for reducing the volume of information for review: we can search by keyword or date or by individual participation, such as all IMs between two users. And the benefits of reduced data volumes and pinpoint relevance determinations certainly extend into the production phase. It's a really powerful capability.

Editor: Is authenticating the tweet or post ever a challenge?

Roffman: Traditionally, this has been true in cases that have gone to trial, and there are two issues we most frequently encounter. First is the fact that social media content is ever-changing, so even if you print out a Facebook page, you may not be able to go back and show the same content at a later time. There may be additional postings, or perhaps the user took down or edited the page. It all adds up to authentication issues.

The second challenge has to do with the motivation of parties engaged in litigation and, therefore, highlights the value of using a third party like FTI Technology. In addition to being independent, we offer the right tools to capture additional information, perhaps about a Facebook post, that can help validate that it was collected properly. We do this by generating what essentially are fingerprints of an individual item, sometimes referred to as a hash value. And when we later present this item, we can demonstrate that it has the same hash value and, therefore, that it's the same item we collected on a prior date. When a reputable vendor makes this presentation, it goes a long way toward resolving authentication issues.

Editor: Are there different privacy

issues involved in gaining access to a website versus to an individual's Facebook account?

Roffman: There are different levels of what we can actually collect. If the information is posted in the public domain, we can preserve it in some way, either by printing or by using software tools that are specially designed for collecting this data. If the information is not shared publicly, we have two options: ask for the user's credentials or, if you have the power, get a subpoena. Clearly, in the latter case, it's helpful if you're the FBI or the DOJ because there are obvious privacy concerns. Facebook is not going to hand over data just because somebody asks for it.

This is an evolving area. So far, the prevailing mentality is that social media is private information, but that attitude is changing and will have an effect on user behavior. For example, setting up a separate account just for business communications will make it easier for the user to hand over data, and some companies have policies that allow the use of social media but also require employees to sign a consent form that allows access to the data as needed. Such policies will change in response to further developments, so it's a very exciting field for us in helping our clients.

Editor: What are the important considerations for legal teams in handling a matter that involves social media?

Roffman: It's never a good idea to be scrambling to figure out how to collect and produce information as quickly as possible, so legal teams should think through these issues and establish social media policies before a matter arises. When facing litigation, the company often has to ask employees for access to their accounts. That's a difficult conversation to have, and in the absence of an effective policy, it's the employee who decides what to share.

Certainly, companies can avoid this problem by having a policy that prohibits employee use of social media for official company business; however, if it's the employee's duty to post things on social media, then the company needs a policy that outlines acceptable content for posts and authorizes individual access to the account.

Needless to say, addressing these issues before litigation arises will limit costs downstream, particularly when facing deadlines during the review and production stages. Everything is more expensive when

there's a rush, so my best advice is to plan ahead, get the right policies in place and then line up a skilled vendor like FTI Technology to collect, cull and help with the review and production phases.

Editor: Are companies buying their own social media collection tools, or are they generally relying on legal service providers like FTI Technology, which offer an array of tools?

Roffman: Companies usually purchase tools because of a regulatory requirement to preserve all data, in which case, for example, they will purchase something that simply collects all Twitter activity without thinking ahead toward possible litigation and the need to search individual tweets. Absent a regulatory obligation, these tools are usually needed in connection with a one-off litigation, and it makes more sense to hire an FTI.

We try to stay technology-agnostic so we can offer the right solution depending on the client's needs and goals. In the case of a one-off litigation, large data volumes might not matter as long as you find one key piece of information, whereas if you're involved in a sweeping e-discovery effort involving 60 social media accounts, then you want to be able to narrow down to what's relevant and push away extraneous personal messages. So our approach is to pick the right tool for the job, and we discuss these issues with clients right at the start of projects.

Editor: Aside from LinkedIn, Twitter and Facebook, tell us about collecting from more obscure sources.

Roffman: We've collected from the private websites of many organizations, and one case stands out for the challenging content it presented rather than for the technical difficulties of collecting from the site. It was a trademark infringement case, and our work involved downloading several videos of advertisements the company made in the 1980s and which had been placed on many different websites and on the company's Internet portal. The fact that they were so scattered posed interesting challenges relating to how web-streaming video is stored and what technologies are available to collect it. These are not typical files that you can just download like a Word document; they stream to your computer and are not saved onto your hard drive, and in this case, they were also 30-plus years old.