The Internet is Forever: Social Media's Role in Claims Litigation - Episode #155

Posted: Thur., July 30, 2019

Hosted by: John Czuba, Managing Editor
Guest Attorneys: Jim Boyers and Robert Simmons of Wooden McLaughlin LLP
Qualified Member in *Best's Recommended Insurance Attorneys* since: 2017

John Czuba: Welcome to "Best's Insurance Law Podcast," the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, Managing Editor of *Best's Insurance Professional Resources.*

We're pleased to have with us today attorneys Jim Boyers and Robert Simmons from the law firm Wooden McLaughlin LLP in Indianapolis, Indiana. Jim Boyers is a partner and trial lawyer who represents clients in complex matters, involving multiple parties arising from product liability, construction, and environmental claims.

His work has included multiple multi-district litigation, or MDL, matters in federal court. Jim often works on e-discovery strategy, including the negotiation of and court arguments about search terms, the handling of data from complex databases, and standing orders for production of such discovery.

Jim also organizes review efforts, including contract reviewers and applying appropriate technology to reduce client costs and to serve their litigation goals. Robert Simmons focuses his practice on the areas of business litigation, product liability, and other civil litigation matters.

Robert also has significant electronically stored information, or ESI, background and e-discovery experience in large-scale, complex litigation, often involving multiple parties, as well as smaller matters where electronic data must be handled effectively at a much smaller scale.

Gentlemen, thank you both very much for joining us today.

Jim Boyers: Thank you, John. We appreciate the opportunity to talk with you today.

John: Today's podcast discussion is on social media's impact on cases. For our first question today for Robert, can you tell us, what is social media?

Robert Simmons: When we think of social media, we think about posting-type media that allows you to place/post [inaudible 1:42] an electronic message into the electronic ether, as it were, where it will reach the public, or some smaller segment of the public.

When we think about that, we think about things like Facebook, Instagram, Twitter, LinkedIn. Within that definition, we can also include instant messaging, or even personal email. Arguably, the listservs from the old days were one of the first kind of execution of the concept of what social media might be.

Where you'd send out an email to a group of people who are interested in insurance litigation, knitting, or what have you, and then they can respond and interact. Social media is rapidly evolving, though.

We've come a long way of the listservs of old. You had MySpace, and now Facebook and LinkedIn are the dominant players. Every day, there are newer apps that are coming out toward this same sort of thing, where you can communicate and share with the public at large, or a group of people that have a shared interest.

Now, we have things like Snapchat, WhatsApp. Some of the lesser-known players that we've seen coming through in litigation are like Marco Polo, Tumblr, Mastodon, Slack. Every day, there's something new.

When you're talking about social media in the context of litigation, it's really important to know your client and the opposition. When you're trying to decide what is social media for your case, it's really important to ask both broad and narrow questions during your custodian interview to figure out what social media is going to be implicated.

The more tech savvy and younger that your clients are, or your opposition is, the more likely you're going to see something that the typical lawyer has never heard of. You may even see things that even seasoned e-discovery lawyers may not know of, just because there are all these new apps that are coming out just about every day.

As a practice point, you're trying to decide what is social media for your case- You're going to make sure that your questioning of witnesses in depositions, and you're drafting written discovery requests in such a way that you catch things that may have not been on your radar, things outside Facebook, Twitter, LinkedIn, and so on.

John: Thank you, Robert. Jim, can you tell us why social media's important in your cases?

Jim: We are looking at social media in almost every case. I think, in some cases, it's more important than others. Folks, when they're on social media, whether they're posting or communicating via instant messenger, email, are often unguarded.

Or, in some cases, they may exaggerate the truth. The bottom line is, with either approach, it gives you open access, if they're public with their social media, to view the implications of social media before the formal discovery gets started.

Also, we can see inconsistencies between what people are saying in their discovery responses and what they've posted on social media. Sometimes, we can see photos and video evidence, and get to know a party before the case is really getting started.

That can help to develop strategy and may give you the opportunity to do early depositions. Another thing we see is people utilizing in commercial cases -- we've seen this in non-compete cases and trade secret cases -- folks using their personal email accounts to obtain and transfer data.

I think they do this based on a false belief that there is an inherent privacy protection for their personal email. If you craft your discovery carefully and target it, you can get the people's personal email and texts.

That evidence can be invaluable to proving violations of employment agreements. Now, certain younger segments, like Rob referred to, may be more careful with email and less careful with text and instant messaging.

The thing there is that a lot of attorneys have argued that text messages are too burdensome to deal with. Courts are a lot less sympathetic to that argument, and the technology makes it much easier to get to that information these days.

Finally, I think that there are sometimes issues with ephemeral messaging. That means people using platforms where messages get deleted. That can present a variety of challenges, and you may need forensic experts to deal with those things.

John: Thank you, Jim. Robert, what ethical obligations do attorneys have with respect to preserving clients' social media ESI?

Robert: You're just talking about the Rules of Professional Conduct 1.1. The key takeaways of the ethical obligations is that in 2019, social media e-discovery is essentially just discovery. We've seen attorneys making arguments that data that resides on Facebook's cloud, for example, isn't within their custody or control, or it's not reasonably accessible, because it's too burdensome.

There's a fair amount of federal case law and a growing body of state case law that really says that those arguments just are not winners. When we start talking about the ethical obligations, we're talking about a duty to preserve, just as you would see for email or paper documents being applied to social media.

Now, where it gets tricky with social media is the privacy settings. We've seen a lot of this where the duty to preserve and the privacy settings that are available to you in social media seem to conflict in some ways.

If, hypothetically, you have a client who's posted something on Facebook that, if they were being a little more judicious, they might not have posted that on a public forum, as the attorney, what can you do?

Again, the core takeaway here is preservation. When we talk about the privacy settings, there have been a couple state ethics opinions that say, "Sure, you can actually have your client increase the privacy settings of that regrettable post, so that it's not in full public view, but you need to preserve it."

A couple have even gone even further. For example, the Florida State Bar said, "You can even delete it from Facebook's server, if you preserve it so that it's available to the opposing party."

That's actually been tested, at least in the Western District of New York, where you had a case where a client had increased the privacy settings from Facebook so that no one can see it.

Their information was still there. It was still available to be produced for a discovery request, so there were no sanctions issued. Beyond that, you have a duty to educate your client about the need to preserve evidence.

There's another case that came out of a district in Nevada where you had a younger client. She deleted a bunch of things from her Facebook. The attorney goes in front of the court once it comes up on a hearing for spoliation and says, "Hey, my client is a younger woman. She deletes things as a normal, in the course of her working with Facebook."

The court didn't buy it. The court said pretty explicitly that once she retained counsel, it was her attorney's obligation to inform her about the duty to preserve and make sure that that was done. The consequence of that was an adverse inference instruction.

More recently, in some of the cases we've dealt with here at Wooden, we've had an opposing party who did not educate the clients on the duty to preserve and all sorts of things went missing, such as text messages, emails, some things in databases.

It's going a little bit beyond social media, but because social media e-discovery is just discovery, the same things would be applied. Because of the wholesale failure to inform the client about that duty to preserve, we got a recommendation for a default judgment.

The consequences for your failing to preserve or failing to educate your client about their role in preserving evidence can lead to some serious consequences.

John: Rob, how do you go about obtaining social media evidence?

Robert: There are a few ways, and it really depends on where you're trying to obtain the data from. I like to think of it in three buckets, client side data, opposition data, and potentially third party data.

Now, as I mentioned at the top of the podcast, courts have pretty consistently held over the last few years that social media ESI, electronically stored information, is within your custody or control, and you are obligated to produce it.

Even though it may sit on Facebook's servers or Instagram's servers, you control it, so it is subject to production. When you're talking to your clients, you want to make sure that you identify all of those sources and not let any of those things that you might need to preserve fall through the cracks.

Once you identify them, most platforms have a self-service download option for a cost-effective collection. You don't necessarily need to do them with a third party ESI forensic examiner or anything like that, depending on the case, of course.

You can consider using that self-service download as a method for snapshot preservation. In the case that we talked about earlier, where there are some things that you might want to increase the privacy settings, you can go ahead and download the entire profile to make sure it's preserved, then adjust those privacy settings accordingly.

Now, the catch with that is, depending on data volume, they can take a long time. A lot of it might not be relevant to the case when you're doing wholesale downloads. You want to plan ahead towards downloads in review.

I know in one case, we had a particularly active Facebook user, where it literally took three days for Facebook to compile the export into a downloadable format. Then to review all that data, it took quite a bit longer than that.

When you're talking about these social media exports, and you have deadlines for production, make sure you take into account that it's not necessarily the fastest process in the world as you plan ahead. The other thing to consider is that some of these social media platforms have this ephemeral data.

Snapchat is probably the most famous example, where messages essentially disappear after a certain amount of time. A lot of times, with these sorts of messaging platforms, you can't delay when you're going to do that collection and preservation if there's important, relevant data that you know is there.

Sometimes, delay can lead to deletion, and that deletion could lead you into trouble with the court. Now, when we're talking about opposition data, rule 34 applies. Just as with your stuff, it's subject to production.

Proportionality also applies. When you're crafting your discovery request, you must be able to articulate why you're asking for what you're asking for and why it's relevant and proportional to the case.

The case law would seem generally doesn't support demanding every single post on Facebook they've ever had or having them hand over their passwords, so that you can inspect their profile. You need to be able to pare your request to be a little more narrow than that.

Another thing to consider with opposition data is preservation letters. This helps you with the ephemeral data on their side. When you send out that preservation letter, put them on notice that these things...For example, their Snapchat might be relevant to the case.

It tells them that they need to collect this pretty soon, and if they don't within a reasonable time after that preservation letter, well, now, you set yourself up for potentially seeking sanctions later on down the road.

Then when we're talking about third party data, you've got rule 45, which is the third party subpoena [inaudible 14:12] rule, which allows you to get a lot of that same data from non-parties. Those non-parties, again, subject to the rule where their social media is within their possession, custody or control, they would have to produce it.

You've also got publicly available posts. For example, third parties might not have the same privacy settings, where they've had an opposition party in a post that you can't see from the opposition [inaudible 14:38] , because they've got the privacy locked down, but you can see it from the third party, who was maybe not as careful.

Now, the thing that you might have to worry about with obtaining social media from a third party is if, for example, they've already deleted this, and you want to try and get the residual data directly from the social media platform. That can actually be a bit of a challenge because of the Stored Communications Act. We can talk a little bit that a little more in-depth.

John: Jim, can you tell us, what are the challenges with working directly with social media platform providers?

Jim: Sure. I'll start with the client. Number one is making sure that you understand each platform and what you can download from it. Typically, you can get that information from the website itself.

You want to be careful when you're assessing, for example, if you're going through it with your client and their login credentials, that you don't inadvertently modify any of the metadata or entries that are already there or delete them.

Then the process of downloading the information, you want to make sure who you want to do that. Do you just want your client to do it and save yourself an extra witness? You, as an attorney, certainly don't want to make yourself a witness to the process of downloading it, but you want to make sure that it's done properly.

That's something to think about. Then when you present it, these downloads often come in HTML files. They don't always look exactly the way things look when you go onto Facebook or otherwise. You need to think through how you're going to present it effectively.

Also, to the extent the metadata's relevant, how you're going to utilize the metadata and present it in court in a way that's acceptable to the judge and the opposing party.

Then, when you're dealing with opposing parties and third parties, Rob mentioned the Stored Communications Act, which is found in 18 U.S.C. §§ 2701. Essentially, if you're dealing with the party who is the account holder, they have control, and they can get to it. If you're running into difficulties or denials of the existence of information, and you want to go directly to the platform, they're going to be limited in what they can share under the SCA.

That means you may be able to find out communications were made on a given day between people, but you won't be able to get to the substance of those communications. If you're going directly to the provider and trying to do a subpoena, there are often very difficult procedures that require you to go out of state to get that information.

It takes time, it takes money, and if you're trying to get some record of deletion of social media, they don't really maintain audit logs for a long period of time. You want to get out there on the front end, get the providers on notice, to ask them to preserve things relevant to your case.

Finally -- this happens more in criminal cases than civil cases, but -- sometimes, there are allegations that accounts are fake, and they aren't the party's account, or that someone got unauthorized access and put fake information on their account. That's something to keep an eye out on and be prepared for.

John: Jim, can you also tell us, what are some common problems with social media productions that you receive from opposing parties?

Jim: Sure. I think, in state court cases, especially, we see a lot of people relying on screenshots. Screenshots may have their place, especially if it's a text or something of that nature, but if it's a screenshot of a photograph, we take real issue with that.

They can be distorted through the screenshot and printing process, and you lose the metadata associated with that material as well. In fact, we recently had a fight in a case that went to trial where we were initially provided printed copies of digital images.

We had to fight to get the original digital images. When we got them, we were able to demonstrate that the photos were, just the printing process in itself, materially altered the photos, and that they had lost many of the digital images that they printed.

Again, when you go down this path, if people don't do things the right way in terms of preservation with social media, you may have a spoliation circumstance. Certainly, it worked for us in that case.

We also see broad objections to social media discovery, arguments of burden from a technological standpoint and from a privacy standpoint. It's important to target the discovery and to be able to educate the opposing party and the court about why it's not as burdensome as claimed.

You have to be able to communicate in a non-technical language what the technology can and can't do. We see that folks are getting more educated every day on the technology side, but it's important to take the time to be as clear as possible as to why you need the discovery you're getting and why it's not so complicated for the other side to provide it.

Finally, I think when you're dealing with productions from opposing parties or third parties, you can't just assume they're going to agree to stipulate as to the authenticity of anything they provide.

It may be that they'll do that, but I think the safest thing to do is to have requests for admissions to help establish the authenticity of anything that you anticipate you're going to use at trial. Don't wait until the last minute.

John: Gentlemen, thank you both so much for joining us today.

Robert: Thank you.

Jim: Thank you.

John: That was Jim Boyers and Robert Simmons from the law firm of Wooden McLaughlin LLP. Special thanks to today's producer, Scott Richards.

Thank you all for joining us for "Best's Insurance Law Podcast." To subscribe to this audio program go to our webpage www.ambest.com/claimsresource. If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com.

I'm John Czuba, and now this message.

Transcription by CastingWords

To find out more about becoming a Qualified Member in *Best's Insurance Professionals & Claims Resource*, contact claimsresource@ambest.com or visit our Learn More page to start the application process.