Social Media Governance: Applied Discovery and Sensei Enterprises put it all in perspective

Jun 25th, 2010 | By Gregory P. Bufithis, Esq.

25 June 2010 — Social Media Governance. A new term creeps across the e-discovery and compliance landscape, seeking to join the pantheon of other irritating phrases like "governance, risk and compliance", "legal project management" and "early case assessment". It seems that "everybody" is doing it.

But although social media is a boon to corporations as a conduit for their communication, it can be a menace, too. As we have reported and as you can read throughout the ediscovery media universe, social media has made discovery even more complex. As Nicholas Adamo of Deloitte Forensic recently noted, you have employees creating information in pockets that are not controlled by general corporate governance policy, on servers that are generally not owned by a company and can often really skirt the edges of a company's intellectual property or relevant business documentation. It's very easy to put something out on Twitter or in an SMS or email that arguably, might be as part of a general business conversation, but when we come back and look at IT and legal departments within a firm, they don't have the same controls over those data sources as they do over their standard email server. So the emergence of those new technologies is significantly complicating a normal firm's capacity to effectively manage an e-discovery."

New research by Deloitte shows that almost two thirds of companies are concerned about the use of social media in their company and its implications for e-discovery. Corporations fear employees accessing social media will result in uncontrolled malware outbreaks, phishing, breaches of confidentiality and trade secrets. Or potential fraud as our coverage of the Societe General/Jerome Kerviel trial revealed.

So it comes as no surprise that two companies that "get it" and are ahead of the curve on all of this (Applied Discovery and Sensei Enterprises) recently introduced a new e-discovery consulting service to help corporations assess, mitigate, and manage social media risks. The service is called "Social Media Assessment, Risks, and Techniques (SM-ART)" and its focus is properly considering the unconventional unstructured data generated from leading social media platforms in support of electronic discovery planning. It has a lot of cool features like an organizational social media landscape overview, an organizational social media actual usage map, a social media risk exposure report, etc.

For full details on the SM-ART service *click here*.

The folks behind it are all experts in e-discovery and social media. Two weeks ago, Valerie Pelton (co-founder of The Posse List) had the opportunity at the 22nd Annual General Counsel Conference in New York to meet with Rob Robinson and Ginger Henschel of Applied Discovery, and Sharon Nelson and John Simek of Sensei Enterprises to discuss social media: the good, the bad, the ugly.

PELTON (PL): First, let's have everybody introduce themselves.

ROBINSON: Thanks Valerie, my name is Rob Robinson. I'm with Applied Discovery. And my role is senior director of worldwide marketing.

HENSCHEL: I am Virginia Henschel (Ginger), an attorney and Vice President of E-Discovery Affairs for Applied Discovery.

SIMEK: And I'm John Simek, the vice president of Sensei Enterprises. And I primarily deal with technology.

NELSON: I'm Sharon Nelson. I'm the president of Sensei Enterprises. And I am a practicing attorney.

PL: All right. Well, I'm glad that you all were able to make it this morning for this conversation at the 22nd Annual General Counsel Conference here in New York. One of the things that we are looking at is emerging technologies and developing and maturation of technologies, particularly in the e-discovery space. And one of the things I wanted to ask you, based on your most recent press release, is about your collaboration and how you came to find each other and what the strengths are that you see in the partnership.

ROBINSON: It's kind of interesting because even though the offering is around social media, our relationship, quite frankly, started several years ago via social media. I had met Sharon and

followed her blogging efforts and then through an understanding of her company's expertise as presented in those blogs, became aware of John. I also know of John from his speaking engagements and his work in "social media". In the past several months we've seen the pulse rate increase on e-discovery tied to social media – so I just thought it was a logical extension of our relationship to find out if Sharon and John were observing the same social media challenges and if they were interested in working together to offer a service that could help corporations and law firms address this challenges in a pragmatic way. Sharon?

NELSON: Yes, I think that's true. And we do deal a lot with security. So we're heavy in the weeds when it comes to figuring out what's going on in a network and how to control it either through the use of hardware or software. And that's, of course, John's specific expertise. And as a lawyer, I bring that perspective as does Ginger Hentschel from Applied Discovery.

PL: Now, John, on the developmental side, what were the things that you were looking at as far as being the most difficult aspects for integration?

SIMEK: Well, I think the challenge that you have is companies don't have total control over everything. So to be specific, people's use of their personal smart phones. That's not a company asset. Short of jamming cell signals, you're not going to be able to do a heck of a lot about it. So your technology choices are going to be far more limited.

And you're going to have to go outside of the normal networking. You can do things internally hardware, software-wise, certainly to monitor data that's moving across the wire. But you've got other challenges there, too, because there's all kinds of ways that folks will try to get around things, even using company equipment, using proxy servers, using encryption. So even if you're doing deep packet analysis, you're not going to see what the data contents are if it's encrypted.

NELSON: And a lot of companies don't understand that. They really don't understand that they don't know what's going on. And as I mentioned to you earlier, Valerie, the *Wall Street Journal* has published ways to get around both hardware and software blocking. Lifehacker has an entire section devoted to getting around it. So what they're doing is they're — whatever controls are put in place — they're all being evaded. And most of the companies are just starting to figure out that we put in these controls and guess what? They don't work. The kids are out. They're running loose.

PL: Now, what do you see as possibly being a negative side, if there is one, if you're looking at specifically the application you have developed? Are there risks going forward associated with using it that you would be looking at either minimizing or trying to channel otherwise, through legislation or other ways to prevent degradation of the service or, development of, competing technologies?

ROBINSON: That's a good question. It's a very broad question. From my perspective one of the challenges I think we'll ultimately face are the risks associated with social media usage. I think ultimately one of the challenges is that no technology solution is the final answer. And if people begin to believe that because they've solved this at a specific point, place in time that it's solved going forward there are not being totally frank about the risk. They may not understand

the challenges of social media. So to have our SM-ART service you can get a free consultation. I mean, you can find out whether it's something the organization wants to investigate more. But you can bring in some experts like Sharon, like John, like Virginia who can add some understanding to the data that the organization may already have and help them make decisions. And one of our pieces is a case study — I don't know if you've had a chance to read it yet – that we sent that around to people who were in charge of law firms. The response was "Oh, my god, I never thought about that". I mean, they really were distressed because now they know what they didn't know before. And now they know, oh, there really is a risk here.

HENSCHEL: For me it started 18 months/2 years ago when Wall Street was going through its meltdown and the Wall Street Journal Journal legal blog and the Above the Law blog – which really got to be something that lawyers read every day — had all these young lawyers leaking information and talking about their firms in derogatory manner. And it was all showing up on these blogs. And I remember saying to my youngest child, who was in one of those law firms "If this ever happened in any corporation I worked in where a single employee did this, it would be tracked down, and they would be terminated". And yet these Wall Street law firms were willing to tolerate associates talking about what's going on in the internal dynamics of the firm in a forum that's going to become public just appalled me. But I think they had no idea how to control it.

ROBINSON: You look at it from a risk perspective. People are looking at social media the way the military looks at intelligence. You know, just because I don't write on my blog something that's overt, I can take a simple post that I make, a simple post Ginger makes, one John makes, maybe something Sharon did on Linked In with a group and string those pieces all those together and those pieces create pictures – pictures that may or may not involve risk.

HENSCHEL: Well, that's what FaceBook is doing with these community pages where they're extracting what someone who works here has said about their employer, someone else's FaceBook. And then they're saying, like, this law firm — they're slave drivers because they have 150 different lawyers in different parts of the country who have all identified that they work for a particular law firm. And then FaceBook draws that out and creates these community pages where they think these people work. They all have a shared interest because they hate their employer and they think that they're not treated very well.

ROBINSON: Which is the contextual piece of it I mentioned earlier. Being able to piece the parts of a lot of these things together and understand ultimately what the risk is in the business world.

NELSON: But it is also balance. We know that there's great promise and great uses for social media. We also know that it presents a serious number of risks from compliance, preservation in e-discovery. There are so many kinds of risks. So a corporation needs to strike a balance. And as Ginger keeps mentioning — but it's the truth – it is training, training, training. And if we haven't said it enough, let's say it three more times because unless you keep that training going, you're never going to have your employees keep up.

HENSCHEL: And I'm sure that less than 1 percent of U.S. organizations have a social media response team to deal with something going virally — already have procedures in place. They have not dealt with what they are we going to do if something gets leaked and they need to retract it or need to respond to it so that we can do something that will impact it all before it goes viral and damages their image.

NELSON: And it is a flash fire when it happens. It really is. But I think in the same way we saw over the last few years all the major corporations having in place a litigation hold plan and a litigation hold team we're going to see a social media action team and a social media action plan. And people are going to start developing all of those as well.

PL: It's like a quick reaction force.

ROBINSON: Exactly. I mean, there'll be a point — I mean, this is a new service. We consider it innovative, cutting edge. But there'll be a point when everybody — this is just standard practice and you wouldn't even think of calling it out as a separate thing. When that occurs, who knows exactly when. But it's going to happen.

HENSCHEL: I think that the changes the corporations went through when they needed to get up to speed on the Federal rules amendments with respect to electronic discovery means they're going to jump on getting social media response teams and getting social media planning teams and somebody who has responsibility for it in an organization. They're going to jump on that much sooner than they did putting together the processes and protocols for doing electronic discovery.

PL: Ok, so do you see the next iteration will be collaboration with advertising firms, people that are used to getting out a message very quickly?

HENSCHEL: Certainly, they'll need to be a part of your social media response team.

NELSON: Yes, absolutely. And, in fact, those are some of the people who we would want in our initial meetings, the people who use social media for good purposes because we need to highlight those, not just the risks.

ROBINSON: From our perspective – since we use social media heavily ourselves – it was obvious there was a business opportunity just because of our profession (electronic discovery).

NELSON: And getting back to the technology, there's no silver bullet. And we're not suggesting that people want to totally block social media, either. We're suggesting that there's a balance to be struck, that they do need to know what's going on in their network. And they need to manage the risks because they can be sued for defamation, sued for trade disparagement, for instance. There are all sorts of corporate risks associated with social media. We've seen proprietary data leak out through social media. There's a hornet's nest out there.

PL: Now, what about governmental intervention? Because the markets that you are targeting are the corporate side and the law firm side. But what about the government side? Because

there are the FTC, the FCC and quite frankly, national intelligence considerations that come in play when you have the social media issues, particularly the cyber-security and the e-discovery use tools being used for data mining and other applications. Have you seen any of that coming into being considered within your own business plans, or are you looking at selling your services into the federal government and weighing what the restrictions on the — on the use would be if you roll that out?

NELSON: I don't think we've gotten as far as deciding where to go after law firms and general counsels of corporations just yet because, frankly, this is a new area. And humility is a very good quality to have at this point. We are at the beginning. And we don't have an application, per say. We have a service and an assessment and a process that we go through. And we have a number of social media policies.

And we really need to hear from each individual client what is it they're looking to do, what are their goals for social media. And many of them want to be educated, which is why we start with a Power Point saying "here's some of the trouble companies have already gotten in". Obviously, you don't want to go there. Here are some of the risks. We'll try to define your risk through John's use of technology and deep packet inspection and all these things that make my eyes glaze over. But they're incredibly useful. We need to determine "what do you have" and "here is what we found" and then say "ok, here is what you need to do." Now where do you want to go from here?

SIMEK: And remember the story will change over time. I think it's the Marine Corps … right? … that said they had locked down social networking, social media only to find it was a real morale squasher. So they've now changed their whole policy. And they now actually encourage usage of social media … in a controlled environment … in order to communicate with family, friends.

But you've got different requirements for different people, as you point out. You've got SEC requirements if you're doing financial information, for instance. So you need to make sure that you're monitoring that stuff and — and even potentially logging it all, depending on what the regulations say. But if you are an H.R. company, you probably don't have those kinds of requirements. So it varies by client.

ROBINSON: I think if people have processes and techniques into place now … addressing e-mail and the like … then our offering is just extending into that. And I use the term unconventional, unstructured data. But it's just those things that people aren't used to looking at. I think we'll agree that we believe people will make – and pardon the marketing term — SM-ART decisions if they have the right information. The challenge is that in this specific space right now there is not really a lot of difference in people's understanding of what constitutes social media, what constitutes communication. And as John alluded to, there the piece of risk for my company may not be a risk for your company based on what you do. Am I being audited by the SEC? Are my brokers being looked at on all their communications each month by a first-level supervisor? A lot of companies don't have that, but they may very well have a different area of risk.

PL: Apart from the obvious applications for anti-trust review and for litigation, where else do you see your services and tool being used?

NELSON: From a compliance standpoint, of course. That's a huge one as you well know from your coverage of the IQPC Compliance conference and the Compliance Week conference a few weeks ago. E-discovery readiness is a huge one. And just managing the data through company policies. They'll want to make sure that they're enforceable, that people are complying with those policies. Right now it's the wild, wild West out there from a corporate standpoint. And the C-suite is very distressed by the fact that they don't really have a handle on what's going on. So there's that balance between you've got legal requirements, you've got a business policy, and then you have the employees and what they want, which you can't entirely ignore. We have learned that companies that block social media have employees who are not happy. So trying to strike that balance between what they can and can't do and why they can and can't do it and how to monitor what they are actually doing and/or control it — man, that's a tough combination.

ROBINSON: It's a potential productivity issue as well.

NELSON: Yes. It's a time suck, that social media. And we know that people … just look at the studies … are doing social network personal stuff every day at work. How much? Hard to measure. That's exactly what we intend to start … measuring.

PL: And what do you hope to gain through utilizing the measurements? Just basically getting employees to spend more time actually doing work? Or are you going to use it as an educational tool in order to bring employees more into the process and get them more involved with making the company successful or controlling their budgets?

SIMEK: I think it's all of those. A lot of it will be based on the level that the company or the law firm wants to take that. I think education will be self-evident based on the assessment that we do. Should a company decide to have us help educate the organization from a social media perspective and what their footprint is from a social media perspective, we can certainly do that. And then based on the expertise that we have from a forensics standpoint and understanding of networking and technology should they like to leverage some of the techniques and capabilities that John and his team have been able to put together, we'll be able to help solve that problem, too. So it is a matter of giving them the ability to help manage and monitor the communications. And then should folks like, we can also do the education beyond just the executive team or the senior leadership.

NELSON: I agree with that. And I really think if you asked me out of the clear blue "Sharon, what's your view of what most companies should do?" I would say they need to achieve balance. And achieving that is going to depend on the company because they are going to have different legal requirements. And some of them are just going to make up their mind in a way different than perhaps our team would want. But the client's always right. So you can try to help them get to where they want to go. I don't believe in clamping down as hard as some companies have. And I think most big companies have now retreated from the total clamp-down, but by no means all of them. A lot of them still try to do a total blackout of social networking.

ROBINSON: Which I think highlights the point of understanding. Really one of the major premises of the service is to be able to deliver an understanding of where that organization is today from a social media usage perspective.

PL: Do you see a trend based on the industry in which a particular company is involved, whether it's defense or computer graphics or medical technologies? Any difference in how those kinds of companies are actually adjusting their policies or allowing use?

SIMEK: I think the major category that really bubbles to the surface today are service industries. So if you're an airline, if you're a hotel, they have employees and groups that actively monitor social media. They're essentially doing damage control, if you will. So when somebody's standing in line and it's taking too long to check in at the hotel and they're tweeting about it, somebody's immediately on that. So that's a big shift we've seen in the last 6, 12 — 6 or 12 months.

NELSON: Yes, and it's huge. I mean, it's absolutely huge how fast they can respond. And Toyota's a perfect example. They had almost no constructive use of social media, nothing organized. And then when the "unintended acceleration" and other events happened they began to really move. And they moved onto Twitter. They moved onto FaceBook. They moved in a number of different places. Have you seen their recent media spluge? They were able to at least stem some of the damage. They did a pretty good job. It was very credible. And that's why social media has its positive side. It's not just a time suck. It's a constructive tool for business.

PL: So which companies do you see as being key innovation partners, if you will, or clients within the industry using e-discovery solutions or smart technologies that you're providing? Which companies would you like to see as a partner as far as them using your tools or developing new tools?

NELSON: I think it runs the gamut, frankly. There are special needs for special kinds of companies. Anybody who is in the health industry, obviously, is really going to need to take a hard look at this. Anybody who's in securities is going to have to take a very harder look because their exposure is so much greater and their compliance requirements are so much stricter. So there are places that have a desperate need to figure this out now. And other kinds of industries, I think, will lag a little bit behind.

But you're finding that the bigger players — I've seen policies from Microsoft and Cocoa Cola and IBM … that have taken the balanced approach that I talked about. And they're pretty much ahead of the curve on some of this stuff. I don't know how deep they've gotten into the weeds, but certainly their policies reflect a lot of thought.

PL: But do you think that's an outgrowth from the fact these are fairly large companies that have a pretty deep marketing and media-savvy team at corporate headquarters? Versus a company that makes tractor parts … John Deere? Not that I know John Deere's social media policy. But are you seeing the media-savvy groups that are always out there with mass marketing as being the real innovators and leaders that are more likely to use these kinds of tools for compliance or adaptation?

NELSON: I think that that's true, that those are going to be the first. There's a whole bunch out there who haven't even thought about this yet. And really, a lot of this buzz has only started in the last 6 months or so. So it really is the beginning. And a lot of the tools — you'll see a lot of claims about hardware and software tools that, quote, unquote, "can solve the social media problem" … don't exist. No silver bullet. We haven't vetted them all, but I don't think there's anything out there that just "solves the problem". This is not one that can be simply solved by technology.

HENSCHEL: I certainly think companies that have already been actively out there with their FaceBook accounts, companies that depend upon interaction with their consumers to build brand loyalty, etc. have been on the cutting edge of making sure that they have very effective social media policies in place and that they do training and that their employees are very aware of what their obligations are with respect to anything they do on their personal sites when they're talking about their employer.

PL: Well, do you think the recent flap over FaceBook security measures is going to cause immediate adjustments or long-term adjustments in your target clients' use of social medial, whether officially or encouraging employees?

HENSCHEL: I think that corporations using FaceBook to boost their brand awareness were always very aware of just how limited your privacy rights were on FaceBook. I think the people who are more affected are the individuals using it who seem to believe that they had a privacy right that didn't actually exist when they're putting information out there. I think that the individual is much more disconnected at understanding whether there's any true privacy or not than corporations who are actively using these social networking site for their branding purposes.

PL: Do you see that as being problematic, this overlap of the private and professional lives with companies … particularly encouraging employees to go on LinkedIn or other social sites and promote the company or promote what they do within the company?

HENSCHEL: I think it's very problematic. I mean, that's why training is so critical because they have to understand what disclosures are necessary if you're putting yourself out there and you're making a comment. Plus you have to be so very careful not to be disclosing anything that you've become aware of internally in your employment that perhaps isn't ready for public consumption. I think it's a very tricky thing.

Often it's better if you make sure that those disclosures only come from those employees who have as part of their job description the authority to say things about the company or its products externally on social networking sites.

PL: Well, I guess the question is — is how do you even monitor that if they're doing it on a private site? We have First Amendment issues that crop up as well. Are you seeing your client companies relying more heavily on newly or differently structured non-disclosure agreements and other kinds of privacy, basically licenses, if you will, for the employees and their use?

HENSCHEL: Yes, that's a difficult area. You can write a lot of policies and put conditions on your employees. And then whether it's enforceable or not, at least you've given them notice as to what's expected and what you expect. But most often employers find out what's going on via a private FaceBook site or other social networking site because another employee is a friend on that site and finds what's been said to be offensive, egregious or violates some regulation they know the company is subject to. And they break it.

So at that point I personally think it's published. If you put it on your FaceBook site and a third party who you've granted rights to view this is the person who then prints it out or forwards it in some manner, then it's difficult to see how it hasn't been published.

PL: Do you think one of the key things that companies should do going forward is really do annual or semi-annual or quarterly training on the social media implications?

NELSON: Without any question. Because what's striking is that the studies show that most of the employees and most of the firms have no idea whether they even have a social media policy. And very few can cite you any kind of chapter and verse. And because social media evolves so fast, I think if you don't do at least an annual training, it's just crazy because this changes so much that you've got to bring the employees up to speed. And one of the things that we show in our presentation is in the early days privacy on FaceBook was so great that what was public was only a little sliver of a pie. And now there's only a little sliver of that pie that isn't public, that is still truly private. So as you watch the pie and watch the pieces change, it's really striking how little privacy there is on FaceBook. And I'm not just bashing FaceBook. It's also true of other social media sites as well. Once you put it out there, you better assume that it's going to appear on the front page of the New York Times or on a billboard going down 95 because — and it lives forever. I mean, now all you have to do is go to the Library of Congress to get all the tweets from Twitter.

HENSCHEL: In fact, trying to get it taken down becomes such a problem. So let's say it's not employment related. Take an example. Perhaps a child has been killed in a car accident. And there have been photographs that have been published and the parents want to be able to take those down so that they aren't circulating. That becomes exceedingly problematic. We've created this social networking where it is impossible for anyone who actually has rights to something that's been put out there, other than cease and desist and legal actions, to really find a way to take it back. It could be in 1,000 places in minutes.

PL: So, John, how do you see your joint product working in this environment with all of these overarching privacy issues, publication issues?

SIMEK: Well, you're going to need a blend, I think, as Sharon said … of the technology and the policy. You've got major crossroads: the internal controls that you at least can do something about, and the external ones where folks who are working on their home computers, doing their own personal FaceBook or MySpace or whatever they're doing.

So you've got a very different approach to each one. You can do things with policy, but you can't necessarily control. There, in fact, are companies, startup companies now that are

professing to be like Google on steroids. And all they're doing is targeting social media. So you feed them your employees' names, and they claim that they'll be the watchdogs. They'll be the ones out there on the Internet looking at all the social media stuff. This is all new stuff. I don't know how effective that any of this is going to be, but certainly it's getting a lot of people's attention.

HENSCHEL: I'm sure there'll be a social networking entrepreneur who looks at the fallout from FaceBook lately and says "well, I'm going to establish a social networking site that has great privacy. And you can come to us in confidence and know that". But hey … it's social networking. You're putting something out there for your friends or acquaintances to see. So there's nothing private about it once you do that.

PL: I think everybody's heard the apocryphal story of a guy goes out, has a celebration, takes a picture of himself drinking on the metro. And then the next day he gets dismissed from his job because somebody was fishing — going fishing through the sites and saw this and considered it conduct unbecoming. So whether that's a real story or not, it could have some very real consequences. If you're terminated from your employment for private conduct, is this one of the real things that you're starting to see concerns about or trying to address with some of the tools that you're developing?

HENSCHEL: Definitely. And that's why the training and awareness is so important because if you're going to find that certain things are outside your conduct for employees, then they have to be very aware of it. They have to have the training. They have to have signed off on the training. You have to have very specific examples. They have to truly understand because you can't just terminate people if they engaged in conduct that they weren't aware that could result in their termination. That just creates more problems, and not just from the lawsuit consequences of doing that, but from the morale of your employees. It's far better if everybody understands. But I think one of the big disconnects we have in this whole area is we see it with judges who don't really understand technology and how data is tracked and kept in corporations in order to comply with the regulations. And then you have employees who have never had training saying you need to understand this about when you're working on our hardware here at the company. You need to understand that every time you enter a password into your private Google account that it is captured. If there was just better communication to say this is really what you have to understand about how data is retrieved and stored.

PL: So do you think part of this also is a generational issue on use and basically pervasiveness of technologies. Somebody in their fifties versus somebody in their twenties, how they use or view the technology and the applications.

HENSCHEL: I think that most of the people I know in their twenties have no idea that when their investment banker is standing at a bar on Wall Street texting that that's not ephemeral, that it is actually being stored in more than one location and will be retrieved in litigation against Goldman Sachs or JPMorgan. I think they have no clue. They're users, but they're not users in terms of understanding the implications of the technology.

NELSON: And they specifically don't understand that deleted data can be recovered from their computers, from their smart phones, from whatever technology that they're using. "Deleted is not deleted" as we say all the time. But they still don't get it no matter how many times we say it. And when the deleted data pops up, they're always shocked. It's like "I can't believe they could do that".

HENSCHEL: I come across it daily. I'll give you an example, just similar to the example that you gave. I was talking to a person who's on the school board in a town. And she said that there had been a bunch of students, females, who were receiving athletic scholarships for basketball who had been at a private party and had been busted for drinking. And they took offense at this, so they took pictures of themselves with these T-shirts that said they were drinking, , holding cigarettes and holding beer glasses. And they posted on FaceBook. And they were told they must take it down immediately or they were in danger of losing their scholarships. They haven't yet gone to these colleges. Before those kids enroll, before they start playing basketball, these colleges are going to look to see what's out there that these kids have been doing. And they're going to lose. Because this stuff can be found.

PL: I think that's an interesting point. A lot of people, particularly in the current economy, are in transition or may be in transition. And from what I've been hearing, a lot of companies before they even will consider doing a phone interview, much less scheduling you to come in and see a live human being, they're going through and doing social media checks to see if this is the kind of person that they want to come into their company or interview.

SIMEK: Yes, a different type of background check.

PL: Yes, exactly … it's a different kind of background check. So it has other implications and uses apart from just you being at the company and working.

HENSCHEL: And even right after you get the job offer — I wrote a blog on that television show, "Hell on Earth." Have you ever heard of it? Well they hired somebody. She got in the cab, and she texted that she had a job there. And that was part of the requirement, That you not tell people that you work there. And so, she was hired and fired in the span of like 60 seconds.

ROBINSON: And that … well … that really accentuates the risk because a lot of times it's not a slow, brewing risk. It's something that goes awry on social media, especially with the viral implications and the ability to transfer data from one conduit to somebody to another conduit to another conduit. You know it's important to understand those risks up front as your decision making made at the same time — the decision on what you're going to do probably needs to be made up front as opposed to pulling together and assessing everything after the fact because of the time component and the exposure based on that time.

PL: Yes, if there's one thing that you want people to know about what you're doing with your smart service technologies and your consulting services and products, what would it be?

HENSCHEL: You can't write effective policies and do effective training unless you have the technical capability to actually assess what is happening inside your organization.

NELSON: We want them to be smart. And that actually — it's more complicated than it sounds because this is not an easy area to understand what's happening within your company. It's not easy to control. And there are counterbalances against control.

So it's a thoughtful process. And that's really what we're about, a thoughtful process from beginning to end. We use some technology, but this is a process. And it's something that I think all companies need to go through at one level or another, depending on size and industry.

PL: Is there anything that you'd like to add, John?

SIMEK: No, I think we've pretty much said it. Building a little bit more on what Ginger was talking about where I see a lot of folks that forget about disconnect. It's not just you taking the pictures. It's not just you posting it. Your friends might be doing it. So they may just have attended the party, right? You didn't actually take the picture. Someone else took it and posted it. So you've got that issue that you also need to address.

HENSCHEL: Or you're 50 years old and someone friends you from high school and then they go and start posting pictures that were taken when you were 17 when there wasn't any social networking.

PL: It was all anti-social networking back then, I guess. I think one of the interesting things to take away from all of this is the perpetualness of data. Years ago before the dawn of time I used to do intelligence work. And if you're in a collection world, this is basically a collection tool. And it can have other applications as well as implications. And I think one of the things if you're looking at new markets going forward is looking at the use by governmental agencies or doing partnerships with private sector and governmental agencies. This would be a natural outgrowth for the smart technologies that you're using.

HENSCHEL: Yes.

PL: Is that something that you might see yourself getting into in the next two or three years?

HENSCHEL: Definitely. You know, it's an interesting thing with magistrate judges who think they become more sophisticated in electronic discovery. They've seen often that with criminal subpoenas, the people who come in and ask for the criminal subpoenas are much more sophisticated. So, for example, they will always come in and ask for GPS data if there are vehicles involved. But when you have a civil litigation matter and theirs is a truck that hits a car, it's very few civil lawyers who will say I want the GPS data on that truck. You would know how long it was driving and where it came from and all of that. So in many ways law enforcement is far ahead of understanding use of data with respect to what it can demonstrate.

PL: Do you see any interlocking of the use of these technologies with RF technologies?

HENSCHEL: Yes. Yes. And that's like the whole geo-based thing, too. If somebody's going to give me a device, I certainly want to be able to disable the fact that anybody is going to tell

where I am at any given moment. But with geo-based, your average 14-year-old wants to know, wants everyone to know where they are at any particular moment.

PL: They want to be cyber-stalked?

HENSCHEL: They want their friends to join them at the mall, which is a whole different mentality than saying "I want to be a little more off-the-grid than that. I really don't want my social networking to be geo-based that any one of the people I know can pull up and see where I am at any moment".

NELSON: And yet look at Foursquare. And that's where the younger generation is. And they do want to know geographic location. And if somebody's close, they want to meet for a drink. They think differently than I those of us who grew up without all this stuff do. And that's part of the problem in the C suites — they tend to be older, too, and they haven't caught up with the younger employees' thinking yet. And it's a little difficult to get a handle on that and balance it with some of the competing interests.

PL: So maybe everybody should have a 14-year-old on staff?

NELSON: Tom Hanks in Big is a pretty good example.

PL: So what do you think will be the next generation on the smart technologies? Where do you see this all shaping in your space?

ROBINSON: Smart technologies like our offering? Where is this all going?

PL: Yes.

ROBINSON: I think the offering will follow the technology, obviously, because our offering is part of an understanding. The time component, the data component is all important to making sure folks understand. The geographical aspect to data, the contextual aspect of data, the storage of data … all very important. It's one thing to have something in context and then have something out of context.

HENSCHEL: And I think over the next — I mean, I hope it won't be 10 years — the next 5 to 6 years we're going to see, I think, a lot of ill-informed decisions in employment termination cases because the judges hearing those cases do not understand the way organizations track, keep, and preserve data. They don't understand it. And so, they're willing to imply a right of privacy that — that is a standard that can't be met at the same time that your organization is subject to regulations that require them to keep data. So we'll have to decide "ok, we're going to require corporations to be in compliance with all these regulations and have all the data that we can reach in as the SEC or the FTC at any time and get that data" vis-à-vis "but at the same time, we can't track everything our employees are doing". We can't have both standards.

NELSON: But we'll morph, though. Because we've got to morph with social media. We've got to morph with the law. We've got to morph with the changes in technology. And they'll be

operating social media from places that don't exist today. And so, we'll have to go wherever they go.

HENSCHEL: And when you talk about educating employees, educating that C-suite is just critically important because when there are people in employment who use certain mobile technologies, the individual executive VPs really need to understand just how long that information is kept and what regulations apply that if they say, well, I really want this to be deleted every 24 hours, that they're going to be unable to have that imposed as a guideline. And so, there's education on both ends. The younger generation needs to be a lot smarter about what the implications of how they're using mobile technology. And people who are making decisions about how corporations are going to track their data need to be a lot smarter about what regulations and requirements actually apply to that data.

PL: Yes. But I think when we're talking we're mainly looking at the U.S. market. This is a global issue. And you've run into data privacy issues, particularly in Germany where their privacy laws are among the most stringent in the world. And you have this overlap where you go to China, where there's not a lot of land lines for private use. It's within a corporate environment that most people have access to these things. Or you go to Korea, and you use these smart phones to pay for everything. And they've been doing that for 10 years. Or you go to the Persian Gulf, and nobody has a telephone outside of the office. They all have mobile phones, and they text or they SMS or they do a myriad of applications on their iPhones and other emerging technologies. We have certainly learned all of this through our European/Asian subsidiary Project Counsel.

NELSON: I totally agree.

PL: So how do you see this within your industry, what the implications are basically on a global basis?

HENSCHEL: Well, we're very active in cross-border discovery issues with respect to electronic discovery and the need for starting to push through some model orders, model transfer data, setting up some protocols. You're never going to be able to comply with the requirements of every country individually. So you work with those individual privacy data commissioners to try to come to a happy medium so that you can get data redacted and anonymized and get it out of the country. But at the same time, we need to have better methods because you can't go to the Hague Convention and wait 18 months.

PL: Which countries do you see as being most important to be, sort of, first movers outside of the U.S. market for these privacy issues and collaboration?

HENSCHEL: Certainly Germany and France. The U.K. is very straightforward. They tell you exactly what you need to do to be in compliance with their privacy regulations. It would be nice if other countries would just tell you exactly what you need to do and spell it out the way the U.K. has. Then there wouldn't be these issues. But when it's very discretionary and kind of always a catch-22, then that's much more difficult. And we're in a global economy with the onslaught of cloud computing. I get this question all the time: "Do you see a particular danger

with respect to privacy regulations and cloud computing?" Well, of course because unless you're the 800-pound gorilla, you don't have a contractual agreement that lets you ask the cloud computing vendor exactly where is my data. Your data is co-mingled. You don't know where it is. So does that mean I have to comply with the privacy regulations of every single possible nation where I have an employee or a server located? It might. It will cause individual nations to think about how we transfer and preserve data.

PL: Do you see any countries in particular countries that you might target with your technologies or roll out to with your applications, perhaps "first movers" outside of the usual U.S., U.K., France, Germany? Who do you see as the next generation, country-wise, or most likely to be the next leading implementers or users of — of the technologies and services? Would it be Brazil? Would it be India or somebody else?

NELSON: Probably the high-tech countries, the ones that already are heavily invested in technology because that's a natural adjunct. They're going to move to and with social media. So Europe as a whole and Canada, plus obviously India, China and the Japanese. Some of these countries are just wedded to technology. The more closely they're wedded to technologies, the more they're going to swim in the social media waters. And they will with their companies as well.

HENSCHEL: All the countries where you kind of missed the industrial revolution so you don't necessarily have a lot of infrastructure, but you have the mobile technical capabilities because you leapfrogged into that century, will be prime, too.

TP: Before we close off this chat, any wrap-up thoughts?

ROBINSON: I think you need to see social media as subset of the overall communication and information delivery mechanism. I look at it as conduits to the customer, the end user. You have all these different conduits. And since you mentioned your military background and intelligence knowledge – you know that in military planning you can't attack everybody everywhere at once. But you have your main areas of interest, your targeted areas of interest. And as a leader understanding you have to understand your resources and risks. So when you have to deploy your resources, which from a legal litigation life cycle perspective may be finite in nature, you can make informed decisions from the social media perspective.

PL: Interesting analogy because as you know this past May they just set up the U.S. Cyber Command — the current and future generation of the electronic battlefield. And you have the military looking at FaceBook and Linked In and Plaxo and god knows what other sites … oh, Twitter.

HENSCHEL: There are certainly certain types of litigation where if you're not asking about social media data and trying to gather some of that in the litigation, you're probably missing the boat. Because SEC investigations, derivative shareholder suits, etc. … all litigation … depends upon who knew what, when and who was it communicated to.

And we are seeing that the untapped reservoir in a lot of litigation is the board of directors and they're going out and collecting data from the board of directors' home computers, mobile devices. Maybe they're looking at their telephone records. But are they looking at their mobile communications, their text messages, etc.? Because when you're trying to show that somebody didn't abide by their fiduciary obligation, I think that social media data becomes extremely significant.

PL: Do you think that becomes problematic as many people that serve on corporate boards serve on multiple boards. And if you're going into someone's private or office computer, you basically may be crossing boundaries of other corporations.

HENSCHEL: I think that's where you bring in your third party neutral — neutral experts who report directly to the court and are anonymizing all data that isn't relevant and using appropriate search criteria to filter out any — there's preserving. With the level of technology we're at now in this field, people who have a lot of experience and sophistication can cull to the point where there's really very little of the reviewing that would violate the confidences of a completely different corporation and different issue.

PL: Do you see this also applying to emeritus or advisory boards as well as consultants providing outside services to a board?

HENSCHEL: Yes, definitely.

NELSON: Third parties, Yes, all the time. Third parties are being hauled in and asked to do extraordinary things. But remember that when they — when the data is reviewed initially — it's going to be reviewed by the parties' counsel before it gets turned over to the other side. So if there's not — if there's somebody else's data and there's something that's not responsive in element, it's not going to be produced. So some of that will be weeded out in the review process as well. But one other point I wanted to mention is that getting social media data can be problematic. It used to be in the old days you could just issue a subpoena, and bada bing, you'd have stuff. But recently in the last several years, the companies have begun — like FaceBook and so forth — to say we are shielded by the Electronic Communications Privacy Act. You can get the data, but not from us. You've got to go to the user. And so, now you have to go through standard discovery process and get the user to produce the data so they have to go to FaceBook and get their own data. And, of course, part of the problem there is you've run the risk of exfoliation, which you always did in the paper world, too. But for some reason when it comes to electronic data, they exfoliate faster. We see a lot of exfoliation.

SIMEK: Well, they attempt to delete.

NELSON: Yes, yes.

PL: That's just when you walk by with a giant degaussing magnet and accidentally step on it.

SIMEK: And you may not be dealing with all the other forwarded messages, etc. that someone else holds. It's in more than one place.

HENSCHEL: Right. Right, exactly, which is another thing that — that people using the technology, no matter how sophisticated they are that use it, don't necessarily understand about the data.

NELSON: The broadcast e-mails that go out company-wide to 40,000 people. And you're just looking for the one person.

PL: The de-duping, tracking down. But anyways, it's interesting to see how this is going to play out. Anyway, I thank you for your time on this and also for going back and talking about the other issues that we've been looking at.

HENSCHEL: Speaking for the group, we appreciate The Posse List taking the time for a nice exchange on the issues.

Gregory P. Bufithis is the founder and chairman of The Posse List and its sister sites The Electronic Discovery Reading Room (http://www.ediscoveryreadingroom.com) and The Posse Ranch (www.theposseranch.com). He is also founder and chairman of Project Counsel (www.projectcounsel.com).