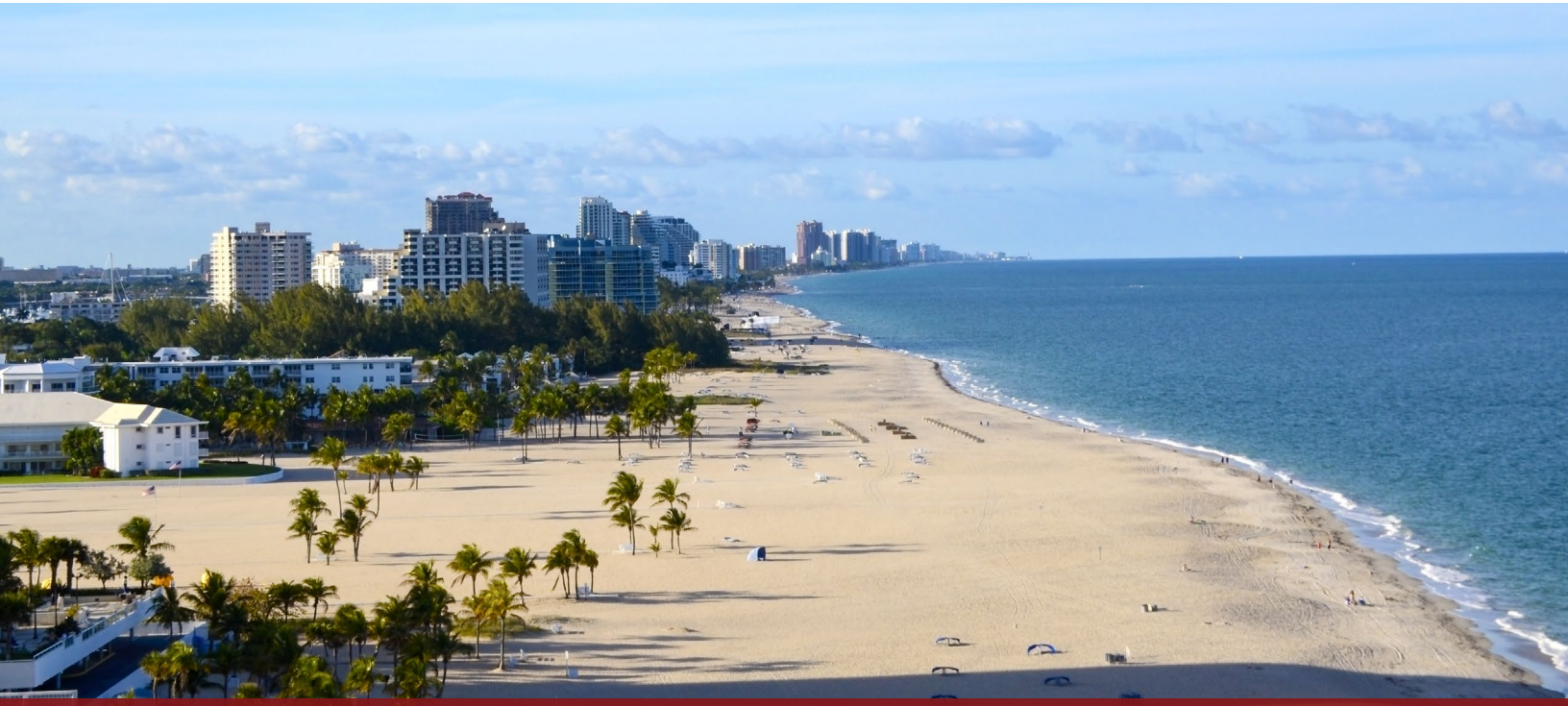
The Impact of Technology on the Employer/Employee Relationship:

Employment Law 2.0



Adapted from a presentation at the 2012 EDI Leadership Summit
Ft. Lauderdale, Florida | October 2012





MAUREEN O'NEILL SVP, Employment Practice Group Leader, DiscoverReady
ROXANE MARENBERG Senior Director, Employment Law, Cisco Systems, Inc.
ABBY HORRIGAN Senior Director, Employment Counsel, Yahoo!
RONALD PEPPE General Counsel & VP of HR, CanAm Steel
SIMONE SCHILLER Director, Employment Law, Integrated Device Technology, Inc.

The Electronic Discovery Institute
www.eDiscoveryInstitute.org

Social Media

Maureen O'Neill: Social media is going to be our first topic for today. I would like to briefly explore the National Labor Relations Board's (NLRB) position on social media. The other thing that the panelists decided that we should do to help make things interactive was to come up with some hypothetical - or maybe not so hypothetical - fact patterns that we would use to tee-up each of the major issues for discussion today.

Each of the issues raise a number of questions, some of them may be obvious, and some not quite so obvious. But here's the first one. The senior vice president for human resources asks you to draft a new policy on the use of social media in a private company and he has a very specific request. First, he asks you to draft one broadly and leave room for interpretation because the NLRB is always changing its mind on the issue. Second, he asks that you draft this policy to make sure that no one is posting false or misleading information on social media, and he also wants you to ensure that non-public company information is not revealed. And finally, he asks that this policy draft include a listing of all of the behaviors that defy their policies. He also apparently has done a little bit of reading because he knows enough to throw out a bunch of case names and he asks that you provide a summary of those cases for him to study up on. Ron, do you have any concerns about the SVP's request, and I'm going to assume that you do because otherwise it would be a pretty short panel.

Ronald Peppe: Since I am the general counsel and the VP for HR for US operations of CanAm Steel, this is one of those cases where I get to tell myself no. You have these great ideas because you really have some tension between the state-of-the-law and its evolution versus what makes common business sense. I don't know how familiar the audience is with the NLRB's recent pronouncements. Has anybody read the memo from the acting general counsel? It was fascinating because they went through a number of issues like this and if you read that memo, it will explain certain things and then it will say, these are illegal. Then it lists another one and says, this is legal. And the average person reading it is going to say, "I don't see the difference here; I can't even see where they're splitting hairs."

This comes up all of the time because of how many people have dealt with a situation where somebody is posting something – typically, a response from somebody who gets angry about reading a post or something that comes up about the company. We have a situation where we put up YouTube videos quite a bit for recruiting purposes. Believe it or not, people find them. We're looking for welders and bidders and blue-collar workers; they come across this and say it's a great place to work. Well, a bunch of employees as well as non-employees started posting comments about what it was actually like to work here, and some of it wasn't true; some of it may have been true, but it may have been opinion.

So, you get into this big debate. The immediate debate for the business people is always, "Let's shut this down; let's find out who did it; let's sue them; I want them banned from the Internet for life." You have to have that talk about the legal side of things as well as the social side of how you can really control it. From a legal point of view, it's becoming pretty clear. The NLRB's position is that you've got to be very specific in your policy to make sure you are not prohibiting conduct for which employees are allowed to engage. And that's, by nature, hard because social media is immediate and it's collective; that's the nature of social media. And at the gist of the National Labor Relations Act, there is protection on concerted collective activity. That's what you have to be careful of. In the Costco case, one of the most recent cases where a big company thought they knew what they were doing, they said their policy was overbroad and it may be construed to prohibit some protected activity. So, it's a very broad test that you have to explain to the business folks.

Maureen O'Neill: What about this tension between activity that may indeed be protected but the company's legitimate interest in protecting its confidential and sensitive information?

Ronald Peppe: Well, that is the tricky part. One of the comments they had was that most of us in the business world know what it means to say non-public and confidential information. It really means something to the Securities and Exchange Commision (SEC). It's almost a term of art. I was in a seminar a couple of weeks ago in San Francisco and there was an attorney from the NLRB there. I raised my hand and said, "How can you give a blanket because their blanket prohibition says it is illegal to prohibit sharing confidential and nonpublic information?" The reason they gave is that salaries and work conditions might be confidential, and non-public, but you can share those. No, that's not what the average person is going to think that means in our minds. But, in the NLRB's mind, they're going to take the broadest most expansive reading of what you're saying and that's when you have to be careful. So you have to take into consideration that anything you put in writing can end up in a court room and you have to think about how it's going to look when they put it on the screen in a courtroom out of context.

Maureen O'Neill: Is one solution to try and create a distinction between the mere disclosure of this information versus what is considered to be concerted activity? Can you help employees understand that difference?

Ronald Peppe: You sort of have to be, and I don't know what everyone else's policies say, but we're a French Canadian company which makes it complicated for us. There are cultural differences as well and there is a policy they issue because they like the idea of one worldwide policy. This is always a problem in the HR front and I am trying to recommend we add examples. We say you can do this and this and this. People used to think that prior case law said that if you put in a saving clause, that meant that you were not going to restrict your rights under the National Labor Relations Act and read it that way. You are going to actually be very specific about examples of what is protected or what is not protected.

Audience Question

What is the scope of this when you say social media?

Do you mean what your employees can and can't do on internal social media for your outward facing Facebook site or another other platform?

Ronald Peppe: It is a real mix and there's a blur. Part of the problem is social media is very individualized. So you've got people with Facebook, LinkedIn, Pinterest, Twitter, etc. And so you've got to look at the media and the venue but you've also got to look at the account owner and who's saying it on who's time. Is there something the company has set up officially or is it something that the employee has set up to do? For example, a couple years ago when we had no budget and we were going through a real downturn in the steel industry, we organized a big get together for managers. We had every employee in the company including all of the managers from around the world get Facebook accounts. We said you're going to sign up. We're going to walk you through it. We want you to put things about what you do and what you do for the company so that when we all get together in Toronto we're going to sit down and have dinner where we are seated based on the interests we put on Facebook. We won an award from some media company.

For a steel company to be innovative, that was good. On the other hand, because we told everybody to go out and get a Facebook account, this gets into the LinkedIn case - is it a company account or is it a personal account? What is the scope of control? Penalty aside from the NLRB issues.

Abby Horrigan: I think there also times where there can be an overlap. For example, Yahoo! has a number of its own social media properties such as Yahoo! Answers where people socialize and ask questions and give answers. I think it gets even trickier when you have a company who's in the business of providing social media outlets. Is somebody who's using that doing it as an employee or are they doing it on their own time in their own account? I think that those are other things that you really need to examine.

Maureen O'Neill: So Roxane, are there things that we can glean from the cases? Are there specific provisions that have formally been approved that are okay?

Roxane Marenberg: Well, the one model social media policy that's been held up, at least by the NLRB, as being the template by which companies should draft their social media policies is that of Walmart. But I'm not sure that if you went line-for-line through Walmart's

policy that it would be consistent, not only with your culture or your employees' wishes, but more importantly, with the company's desires.

There are also a couple of themes. One is what the employees' perception is going to be. In other words, it's not the company's prism through which the policy is going to be viewed. It's viewed through the prism of an employer - they feel as though their rights have been chilled or there is a risk of misinterpretation by the employee of what you're telling them they can and cannot do. Another theme is one of talking about other employees or talking about something that can affect terms and conditions of employment. Those are chilling rights if you restrict them in any way, but some of these cases get down to the minutia of a policy that says you can't walk off the job. Now, you and I might think that this seems to be something that has nothing to do with social media. Why should you be talking online about walking off the job? But again, it was a case that seemed to chill the rights of an employee. When your general counsel or your SVP for HR has drafted the broadest policy possible because they want to make sure they cover everything now and into the future, that's not the direction you want to go.

You want to make sure that you keep reading these cases and looking at your policy. It doesn't mean you're going to be changing your policy. If you were to do so, you'd be doing it every week depending on the cases that come out. The predominant thinking is that this is at some point going to be resolved by the Supreme Court or some court that's going to give us direction other than just opinions from the NLRB. If you look at the policy, the company is concerned about proprietary confidential trade secrets, you draft it succinctly and narrowly and you're not directing an employee not to talk about how he feels or his opinion about the work-place. Again, as Ron said, it's a real fine line. He might really be upset about a product that you're putting out or that's in development stage and you, as a company, as an in-house counsel, say, "wait a minute, it's really important for us not to have that spoken about."

Ronald Peppe: In most employment law situations you're dealing with something that happened - allegedly something happened and it was either right or wrong. For folks who don't do traditional labor law and don't deal with the NLRB, the foreign concept that we're dealing with here is this idea of chilling and preventing something...

Roxane Marenberg: ...that has not occurred.

Ronald Peppe: It's almost as if you're being penalized for what might happen based on some interpretation.

How Does Your Policy Ever Get to the Attention of the NLRB?

Roxane Marenberg: What caused Walmart's policy or Costco's policy? How did they ever get before the NLRB for the NLRB to have an opinion on whether it chills employees' rights? I think the prevailing view is that none of our policies are ever going to get the attention of the NLRB - hopefully. It's not the first agency that an employee is going to go to if they've got a dispute with their employer. They are going to go to the Equal Employment Opportunity Commission (EEOC) or to the state regulatory agency. They're not going to go to the NLRB. But, with that being said, monitoring your policy is so important because at some point there's going to be an employee that's going to misinterpret it and say, "I want to go and put this out there." The thing that is clear from these cases is making sure that you, as in-house counsel, get a chance to have an opinion on whether someone should be terminated or adverse personnel action should be taken against someone who has violated the social media policy. The sooner you can inject yourself into that process the better. You don't want to hear after the fact that somebody was just terminated because they violated a social media policy.

Audience Question

When it comes to the disciplinary action or termination of an employee do you ever look at the intent of an employee who tries to go out and put something in the social media atmosphere who might have created a false account?

Ronald Peppe: The opinion actually addresses that and they get into one of the policies they basically said that it was illegal to say things that are inflammatory or defame people, and it also listed the intent to do things. The answer was that employees have every right to attempt to cause problems for the company or the people if they're doing something wrong in the exercise of their collective rights, which is not something you would tend to think. You would tend to think they were trying to do something bad or for some other purpose.

Roxane Marenberg: They have a right to be a whistleblower.

The Expectations of Privacy in the Workplace: How Technology is Impacting the Employer/Employee Relationship

Maureen O'Neill: So, for instance, you receive a call first thing in the morning from the head of the safety and security department who tells you that he's just received a call from the local office of the Federal Bureau of Investigation (FBI). According to the FBI, one of your employees has been soliciting sex over the Internet from someone whom the employee was led to believe is a minor, using a company laptop with an ISP traced to the company. In the call with the safety and security director, the FBI asks the company to do a number of things:

- Image the employee's hard drive, including the cache history on the web browser.
- Monitor this employee and search his hard drive immediately for anything related to child and adult pornography.
- Ask that they provide copies of his or her travel and expense reports, personnel files, and access to their online Outlook application.
- Place a concealed camera in the employee's workspace so that it can see or record all of the calls he makes relating to the investigation.

The reason for those requests is that the FBI believes that he or she may have been traveling to visit one or more of the minors they were communicating with. Now, if that wasn't a bad enough start to your morning, you find out that that very afternoon the FBI agents are going to be coming to your office to talk about to the investigation.

So after you stop swearing and you pour yourself that first cup of coffee, what are you going to do? What's your plan of attack for dealing with these requests? Certainly the employee does have some expectation of privacy in some of these areas but that's not going to be dispositive of the issues, right?

Abby Horrigan: I have explained repeatedly to safety and security that we always want to cooperate with law enforcement, but our place of business is not 1 Police Plaza. And so the police do not get to walk in and do whatever they want on our property. My first counsel would be to look at what your company policy says. What was the employee issued on the start of their employment that informed them about what we electronically surveil? So if we have cameras, do we have cameras in common areas? Did employees sign an agreement upon the start of their employment acknowledging that they understood that they could be videotaped or audiotaped on our property? But even then, as an employment lawyer, I would not allow them to install cameras. I would not allow them to record sound - certainly not without a search warrant. I would say, "You need to go get a warrant and we will discuss in court about what the requirements of that warrant are going to be. Now, you can search anything you want with a warrant." Go get a subpoena. Now, with regard to the company laptop - this is something that Yahoo! unfortunately has had to be very vigilant about as a company given the nature of what we do. But, we have a legal obligation, everyone has a legal obligation if you uncover evidence of child pornography on an employee's computer. You have a legal obligation to turn that over to the National Center for Missing & Exploited Children, or the FBI. You also have an obligation to call legal authorities if you find this on somebody's computer. So, what we would probably do is run a search of our own laptop and if we find anything incriminating, as required by law, we're going to turn it over to the FBI. That way you don't get into the Fourth Amendment issues. We would do all of that without a subpoena.

Audience Question

Going back over what you said, you'd tell the FBI to get a subpoena – Do you mean the search warrant?

Abby Horrigan: Search warrant, subpoena, yes. I usually deal with civil. So yes, a search warrant. And we would probably go to court and talk about what's reasonable. With regard to the hard drive, there's a lot of our IP on there that I don't want to turn that over to the government for no good reason. I would prefer to go work with the FBI. I want to give them what they want, but our IP has nothing to do with this, and so I want to limit what we turn over to the incriminating evidence, and we would work that out with them.

Maureen O'Neill: Do each of your companies have a policy with respect to at least company hardware and software where employees are explicitly told they do not have an expectation of privacy in anything that's found?

Ronald Peppe: Yes.

Simone Schiller: Absolutely.

Ronald Peppe: You know, it's funny because even most of the HR people think that as long as they sign that statement which says you have no expectation of privacy, the company is protected. It's in almost every employee handbook you see. All the templates have it. But there is also case law now restricting that. There was a case in New Jersey - I know they pulled way back. We got sued in federal court in New Hampshire. I spent a lovely Labor Day weekend in Concord, New Hampshire because it got adjourned over the weekend. I had to come back because we searched somebody's hard drive and their emails, and it turns out the individual was communicating with his lawyer about suing us.

So, you could see that in some of these personal situations there's a fuzzy line between what you can and can't access because they think if they're going online to email - for example this guy was using his Yahoo! account - they are protected. We didn't have a right to see that, even though we could actually track everything. There's a gap between what you can do. Even if you get the employee to sign off, some of the courts have said, "Well wait a minute, what's the real expectation?" They think they have a password and you can't get in there, and then you get into the Stored Communications Act and the other laws that deal with the stuff in transit. Then you've got the whole attorney/client privilege issue which would be fascinating in a criminal case if he already knows he's in trouble and is talking to a lawyer about it.

Audience Question

So how would this analysis change for you if this employee was sitting in Frankfurt or London or Paris or Tokyo?

Simone Schiller: It would definitely change because the data privacy rules are different throughout the world. They're very tight in Germany, Italy, and France.

Abby Horrigan: Isn't it actually illegal to fire anyone ever in Germany?

Simone Schiller: I don't know about Germany, but definitely I'm dealing with some situation in France as we speak. So yes, I'm loving it. In Germany, I'm not an expert in data privacy around the world, but I do oversee it. I would definitely recommend engaging with local counsel experts and working with them. A lot of times you really can't do what you want to do. Okay, so what can we do? Can we manage performance? Is the code of business ethics being violated in some different way? Is the code of business ethics going to stand up? Is it translated? Or do you have one code of business ethics for the entire world? We have one for the entire world, so it may not technically comply with everyone.

Ronald Peppe: In Europe, on one hand, you have the same problem with the whistleblower law. The EU has laws that supposedly go back to the history of Germany and the Nazis and people telling on each other; there's a cultural issue. In France, it's the same way. On the other hand, when you violate these things here in the U.S. we tend to think of it as expensive class action. Over there, you sit down with the regulators and you work through it the first time it comes up. There is not a private right of action quite the same way we think about it. It can be expensive, but it's also something you can work through.

Roxane Marenberg: Right. They issue indictments and take you out of the office in cuffs, but all of this is

an issue in the U.S., I don't want law enforcement, whether it's someone in a uniform or not, going through any one of our offices or cubes. So, we want to cooperate. We're good corporate citizens, and we need to make sure that we maintain a good relationship with law enforcement and any of the regulatory agencies. In this situation if law enforcement came to us and said, "We have credible information that one of your employees is engaged in criminal misconduct," we are going to cooperate.

So, how can we best do that? Could we do the monitoring ourselves? Could we put the cameras up that are compliant with our culture and also our code of business conduct and our employee resource guide, which informs our employees as to what we can and cannot do relative to their space? Do we want to make sure that we protect or recognize the privacy rights of an employee relative to communications with his lawyer, with his doctors, etc? We're not going to look at email and communications that have nothing to do with the relevance of the investigation at hand. So what is it? They don't want to come on to our campus and route around things if they don't have to. If they can have a cooperative corporate attorney deal with them and get the information that they want, they'll be fine. Look, the last thing we want in our workplace - or any of us want in our workplace, I suspect - is someone who's surfing the net and communicating with a minor or someone they think is a minor. Bottom line, that's not what we're in the business of doing. They ought to be creating better ways for the world to live, work, play, and learn. The sooner we can get rid of this issue the better. Most importantly, are you treating your employee fairly? Are they put on notice that they have an obligation to do their work and not to engage in criminal or civil misconduct? And the third issue is whether we are being a good corporate citizen by cooperating with regulatory agencies and law enforcement.

Audience Question

We've talked a lot about protecting employees' rights, but is there a component where his actions have made the company now liable?

Roxane Marenberg: And there was a case where an employer did not get the employee out of its workforce in a timely fashion and the employee then continued to communicate with some other child engaged in child pornography and that family brought a lawsuit against the company. So it's a matter of due diligence. Being informed and acting as expeditiously as possible once you are informed.

Audience Member: That's the crux of my question because the FBI in this scenario is asking you almost to set up a sting operation saying, "We want you to help us catch him, and while you're helping us catch him, you're facilitating the process of his illegal activity." Couldn't that make the company even more liable?

Simone Schiller: As an employment attorney you use the same concepts. If there's an internal complaint about an individual or an executive engaging in alleged inappropriate behavior, it needs to be prompt. You need to take prompt action and it needs to be thorough. You need to just take those same concepts: be prompt, be thorough, and work with the FBI swiftly. Take a route you can negotiate with the FBI. I would not let them put cameras in our workplace. No way.

Ronald Peppe: That's a subject of bargaining. If you're unionized, you can't even do it. You'd be opening a whole can of worms there.

Simone Schiller: I would not, but maybe I would offer up the use of our own cameras. If an employee complained about this and maybe discovered this or walked by his computer and saw something, how would we handle it? You do an investigation. So you do the same thing. It's the same protocol. If you would use a camera normally, where would you put it? If it's a cubicle, sure, maybe put it in a cubicle. Look at the email. You really need to be prompt.

Abby Horrigan: Depending on the severity of the allegation - and this is pretty severe so in my mind it would fall in that category for me - with certain investigations depending on the behavior that is alleged, we would immediately walk to the employee's cube, and say, "We have an issue; we're going to conduct an investigation; we're going to put you on administrative leave while we do that investigation; please leave your laptop and Blackberry."

Roxane Marenberg: Unless, of course, you were told not to by law enforcement.

Maureen O'Neill: Part of the contention is that the FBI

might come to you and say, "No, don't fire him just yet. We need some more evidence." And you're thinking, "well, if I facilitate this individual contacting another minor or doing some sort of internal conduct that qualifies as harassment - we've now exposed ourselves."

Ronald Peppe: Plus, you don't know if it's true. You run into this situation all the time. It's never this clear. Quite often a lot of these investigations usually come down to just plain porn and then you get into this interesting line - were they under age or were they not under age and what's the liability reported? In every case I've had - and this comes out in eDiscovery, even in plain eDiscovery - there's something routine that comes up. You've got to turn over all the documents, and there are a couple of employees who really push back and say, "you're not getting my documents." It's always because there are negative pictures on their laptops or evidence about something they don't want you to know about. Then, you find out step-by-step. This is why you have to have these investigation protocols so everybody gets treated the same and it doesn't look like you're picking on certain people while using different standards.

Maureen O'Neill: I assume that in this hypothetical situation you've now been put on notice of a potential search warrant or a civil subpoena, some kind of lawsuit. Are you going to put a preservation hold on this stuff?

Ronald Peppe: Well, you may take action. This is where the technology is changing. It used to be everything lived everywhere because that's how it worked. Laptops were independent. Now you've got easier ways of feeding everything into one place. You can make sure it's backed up and saved. Then it's a question of what your obligation is and how far you have to go at that point.

Maureen O'Neill: So again, do you now have an obligation to go hunt down every copy and make sure it's turned over and not retained?

Abby Horrigan: I am going to run across the hall to our law enforcement guy who does law enforcement for Yahoo! and say, "Mattson, help!" I think this is one of the situations where you are not an island and you're going to reach out to one of your colleagues who may know more about this than you do and ask for help. I think there are so many different ways you could approach this, and I don't think there's one right answer.

Social Networks: How Employees Are Using Social Media as a Part of Their Job Function

Maureen O'Neill: Whether an employee wants to use social media or whether they do have a legitimate need to use it, they want to be out there doing it in the course of their job. So this hypothetical situation comes to us from a staffing organization, who asks whether they can use information that they find on social networking sites in connection with their recruiting efforts. They tell you that everyone - I love that, "everyone" - is finding great candidates on LinkedIn and Facebook. Plus, you can learn so much about these candidates by Googling them or by connecting with them on one of these sites. When you get this request you decided that you should have a training session with the staffing and recruiting teams to address the issue. Simone, I want to let you take the lead on this one. What advice are you going to give the team when you get together?

Abby Horrigan: Simone, before you start, I would just like to say as a point of fact, you could also find a lot of information on Yahoo! about them as well. Not just Google.

Simone Schiller: That was fantastic! So, this has come up. We have our staffing team recruiting candidates. They are using LinkedIn. I don't know if they're using Facebook. If they are, I don't know about it. And yes, there are problems that come up. Obviously, I tell them that they cannot take somebody's picture into consideration. Don't look at people's pictures. Please don't Google people or search for people on Yahoo!, Google, Bing - they do it anyway. This is what we need to be honest about - they're doing it anyway. My advice is that you cannot be taking pictures into consideration. You're just opening up a can of worms that you don't want to open up and it's frankly not related to the job.

Maureen O'Neill: So let's make it a little bit messier because as Simone points out, they are probably going to ignore you anyway. So sure enough, a week after the

training session one of the recruiters calls you and says they found a great candidate on LinkedIn. The candidate is located in New York. The job is in California. The candidate's interviews go well. HR sends them an offer letter and the proprietary information and inventions agreement. The candidate executes all of the relevant documents, accepts the offer and sends everything back to the company. A week before the candidate is due to start and has already moved to California, the recruiter happens to be surfing the web and sees that the candidate has a Facebook page but it's accessible only through friends. He realizes that they have a friend in common though, and of course with the memory of Simone's great training class already gone, the recruiter decides to friend this candidate through their mutual friend. Now that he has access to the page he sees pictures of this candidate smoking dope, chugging beer, and getting a lap dance at a gentlemen's club in Las Vegas. The recruiter is appalled.

Audience Question

Are these bad things?

Abby Horrigan: Not in California.

Maureen O'Neill: So, the recruiter's horrified at what he's seeing and he contacts the hiring manager to share it. The hiring manager says, "Yes, I agree with you. I'm appalled as well. We need to withdraw this offer." The recruiter then calls the employment lawyer and says, "I'm kind of concerned about this. The hiring manager is going to rescind the offer but this guy is about to start his job in California. What do we do? Do we withdraw the offer? Shouldn't we withdraw?"

Simone Schiller: I would tell them they cannot withdraw the offer. The candidate has already turned in notice and has left their prior employer. They're already relocating across the country and it's a week before this person's start date. And you're just opening up yourself for a lawsuit. They've relied on this offer and they're moving their family across the country.

What considerations come into play? Maybe it would be different if the person did not turn in their notice yet. If they didn't relocate yet. There still might be potential exposure. I know one of our panelists, what they've done in the past is actually offered a release agreement at 90 days to pay the candidate.

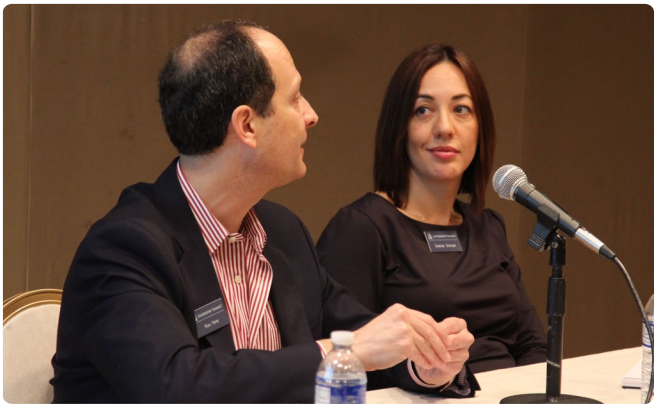
Abby Horrigan: Before we move on, though, another of the considerations that come into play is the location of the employee. We have a very California-heavy panel here, but California has a law that says you can't discriminate or discipline people for engaging in unlawful, off-duty conduct. Meaning that if an employee has a prescription to use medical marijuana, their employer cannot discipline them on the job for engaging in lawful off-duty conduct in their own personal life.

Maureen O'Neill: What if it actually turns out that it wasn't pot in that bong, it was tobacco in a hookah.

Abby Horrigan: What if it's something legal like salvia? If you're smoking salvia out of a bong there's nothing illegal about that.

Simone Schiller: It's not related to the essential function of the job. So there's no tie there.

Roxane Marenberg: So let me just push back for a second on all of this information that's out there about people. Regardless of whether it's appropriate to be looking at it, we know that's the new normal. Everybody's looking up people on all of the social networking sites, including Yahoo!, but some of the information, believe it or not, is erroneous. Pictures can be photoshopped. So, what you see might not be a bong, and that might not have been a lap dance. There's so much misinformation out there. I have been faced with, mind you not in this scenario, information that someone had a prior conviction or a prior SEC consent decree, and it didn't come up when we Google'd or Yahoo!'d someone. I know this is going to sound so self-evident, but the



best thing to do is to pick up the phone, or have your recruiter or your hiring manager call the person, and say, "This is of concern to us. We are a company that has a certain culture and we're concerned that some of the information that came to our attention is inconsistent with our culture, and you may not be set up for success here as a result of this information that's come to us." Give the person an opportunity to explain it away. There is a possibility that the information is inaccurate, that the story about the person having engaged in misconduct, or having been arrested, or having been subject to some criminal investigation is inaccurate, or it's not really a picture of the person at a gentlemen's club.

I don't know what the explanation would be, but you can see that there might be some innocent explanation that wouldn't change your opinion about the individual as a good hire, as opposed to enforcing some kind of a release. The fact is, he may not sign that release. You may have false information about the individual, and I think I'd want to be really sure before I said, "Turn the truck around and go back to New York!"

Ronald Peppe: Well, heaven forbid you had a pattern of doing this and it affected a protective class somehow or there was a disparate impact. For example, if you look at some of the new guidelines against looking at criminal history. You used to be able to at least consider convictions, and now they're saying "disparate impact." The technology also plays in here, because everything is tracked down to the "nth degree". Eventually, somebody is going to come up with a case on this.

There is also a generational issue that has to be managed in the workforce. I once had a boss who wanted me to fire my legal assistant because one day she was a little too unbuttoned and he saw her tattoos. There's actually case law saying you can fire people for that. There was a Costco case in California, and this would apply to piercings and things as well. But you've got to manage that expectation too. So you have to step back and use a little common sense. I always try and say, "It's not just what the law says - maybe we can get away with doing this if you want to do it - but let's think about WHY you want to do this."

Roxane Marenberg: What's the right thing? There have been stories where someone walks by a cube and sees a new person's name up there and says, "Wait a minute, who just hired that guy? I used to work with him in another company. He's not collaborative. Can we not hire him?" Well, yes, in California, if he hasn't moved across country and we don't have a detrimental alliance case, you can withdraw an offer. The case law says you can withdraw an offer before someone starts. However, is that the right thing to do or is there another way to determine whether he was collaborative in this job? We have a 90-day provision, whereby, managers are supposed to get back with the employees at 30, 60, and 90 days and tell them how they're doing. If they're not collaborative, you're going to find that out in 30 days as opposed to not getting talent in the workplace because someone walks by and sees his name and remembers from another job that he wasn't collaborative.

Maureen O'Neill: Let me ask another eDiscovery related question about preservation with this scenario. Recruiters are probably going out there and they're using these sites even if you tell them not to. What kind of trail are they leaving? Are you able to somehow lock it down, if in fact you get wind that someone is bringing a suit of the kind that Ron suggested - in which they claim that you're relying on some of these things in a discriminatory way?

Ronald Peppe: They're usually not doing screenshots and putting them into a paper file anymore. Although in most HRS systems - when they're sourcing people - they will put down the source and track that, so there is a record. I suppose if someone wanted to really get elaborate you could most likely find some sort of history of where they're going and what they're looking at. That's probably how you build a case.

Abby Horrigan: I get screenshots at least once a week from somebody's Facebook page. Employees love to screenshot other people's stuff and send it along. "Look at what this person's doing." But other than that, I'm with Ron. I just don't know -- I'd go with the dispositioning of the candidate and then go from there.

Ronald Peppe: This brings us back to having a document for hiring policies. The government has some great standard hiring practices. You also have to be able to demonstrate that you did it. This might be part of that documentation.

Roxane Marenberg: When you mentioned though, Maureen, the issue of a third-party vendor, the question is, "What records are they keeping?" I think it's important for us to look at our contractual arrangements with these third-party vendors to see what it is they're doing, and what they're retaining. Ron says, if we're a government contractor, there are documents that we must retain for purposes of review at whatever intervals they wish.

Ronald Peppe: Some of these providers offer this. I get calls all the time from CareerBuilder or Monster and they offer you a package where they'll be tracking access, they'll prepare statistics for you and they will preserve. On the other end of the spectrum you've got Facebook that says you can't give us a subpoena for information because we're not in that business.

Information Security: Challenges that Companies Face with International Employees

Maureen O'Neill: Now employees are distributed across the world and are fairly routinely carrying around sensitive and confidential information on laptops, tablets, phones, and on portable storage devices that are getting smaller and smaller and smaller. So, for instance, you learn that a U.S. based employee has posted confidential information about an upcoming product launch on his Facebook page. This employee is on the launch team and is privy to confidential material. You also are concerned that other members of the team who are located in China and Germany may have treated similar information as cavalierly as the U.S. employee. To make matters worse, a blogger has already gotten hold of the rumor and he has called the PR department for a comment. All right, Ron, would you like to talk about the U.S. employee first? What would you recommend? Would you consider terminating him immediately? Would you consider filing a lawsuit and going after this guy as the business leaders want you to do?

Ronald Peppe: This is one of the few times the business leaders will love going to the lawyers and saying, we can get a legal action, we can fire somebody, we can have stuff taken down that they put up. This is when you have to have that talk about how much money will be spent. Although there are some challenges there, particularly on the international side. The reality is that you need to manage this as a whole – you've got to step back and deal with the immediate issue, but then talk about what our policies are, how we manage expectations, and what's the best way to fight fire with fire on social media. You've got to impress upon people why it's important for them to keep certain things confidential and why that's important for the company. It sounds easier than it is, but it's a process.

Maureen O'Neill: Right. With respect to the employees who were in China and Germany, we won't spend a whole lot of time on that. It's fair to say you're going to want to get experts on the ground in those jurisdictions to find out.

Ronald Peppe: Just like we're having our issue with the NLRB and what we can say about posting, you can end up with criminal issues. Our general counsel in Canada cannot go to Mexico right now because there is an indictment out for issues because there was an employee dispute over certain things and that's how they force the matter.

Maureen O'Neill: The business leaders also want to know: Can we have someone go out and actively monitor the web to see how wide the leak is spreading and what impact it is having on us? From the employment law perspective do you have any concerns about that? Do you think that's appropriate? Is it going to impact your decision on what to do with the employee who started the leak?

Abby Horrigan: We were actually talking about this just earlier and about tracking things internally and Ron was sharing with us that there is software that allows you to visually see where information is going.

Ronald Peppe: Is anyone using mapping software? Because it's actually used in eDiscovery as well and it's partly how some of the predictive coding works. It determines who talks to whom and who they typically talk to. You can actually do a visual map of who's connected to whom and highlight who's really got a lot of information so you know whom to focus on when you're doing this kind of investigation as well as to really see where the information is actually dwelling from.

Lawyers like to have things labeled and to write a policy saying that everything is going to live here. You have to store it here. You have to delete this here. The reality is it doesn't work that way. Things don't get deleted.
To track things down, you really have to figure out where the information flows and where you need to focus your efforts on finding things. That's what some of these tools that I've looked at actually let you do. It lets you at least get a much better approximation than the anecdotal evidence about who's connected with whom.

The ADA: How Employers Can Leverage Technologies to Help Provide Accommodations for Employees with Disabilities

Maureen O'Neill: Our fact pattern here is this: You as a lawyer decide that, with the ever-increasing number of claims for accommodations, we want to work with the HR department to put together an accommodations team, which is going to consider a rule on employee requests for accommodations. You also decide that you want to put together a playbook for this team, which is going to drive consistency for that team's decision-making. Roxane, why don't you walk us through this one and talk about some of the initial decisions you're going to make. Who goes on this kind of team? What's going to be in this playbook? How do you assume you're going to deploy this playbook in making decisions?

Roxane Marenberg: I think that there ought to be an interactive process for any request for accommodation - whether they use the term "request for accommodation" is irrelevant. You need to be on the lookout, and have your HR managers, and whomever else are your people on the ground, making sure that if there is a scenario where someone wants to work but just needs an accommodation in order to perform the essential functions of the job that there is an opportunity for there to be interaction. For there to be an attempt to try to figure out how we can get this person doing their job that they had before they fell ill or they needed the accommodation.

We've been very lucky because we have a chief medical officer at the company. We don't do pretesting for and we don't obviously have heavy equipment - we're in the technology area, but we do have a very sophisticated healthcare facility on a number of our campuses. We have a chief medical officer, and she's on the accommodations committee. We have the medical prism through which these requests are being made, but most importantly, it's making sure that you've got a policy in place and you adhere to it consistently. This team has to include someone from the business, because you as in-house counsel or outside counsel aren't as familiar with the essential functions and what goes on on a day-to-day basis. The job description may be totally irrelevant and may have nothing to do with what happens in the workday from 9 to 5 or whatever the hours are. Someone who knows the job, someone from the medical field, someone who knows the ADA from a legal standpoint.

Ronald Peppe: We're back to "reasonable accommodation," and what is "reasonable." Certainly as the technology gets cheaper and more widespread, it's pretty hard to put up an argument that people can't work remotely. It used to be no we can't spend $20,000 to set you up with a nice Cisco System to do this and nowadays some of you can have a laptop and Skype or even an iPad with FaceTime and get in. So you really don't have that argument no matter how big or small the company is. The business people don't want to hear it.

Roxane Marenberg: In technology companies it's going to be pretty hard to say that it's too expensive or that it's unreasonable.

Maureen O'Neill: I think the answer to that ultimate question at the bottom is yes. If you're a high-tech company, you're probably held to a bit of a higher standard than someone else.

Abby Horrigan: Cisco has an amazing Telepresence feature.

Ronald Peppe: And it's not always Telepresence, sometimes it's setting them up so that they can have the technology in the workplace to do the job.

The 2012 EDI Leadership Summit A-List

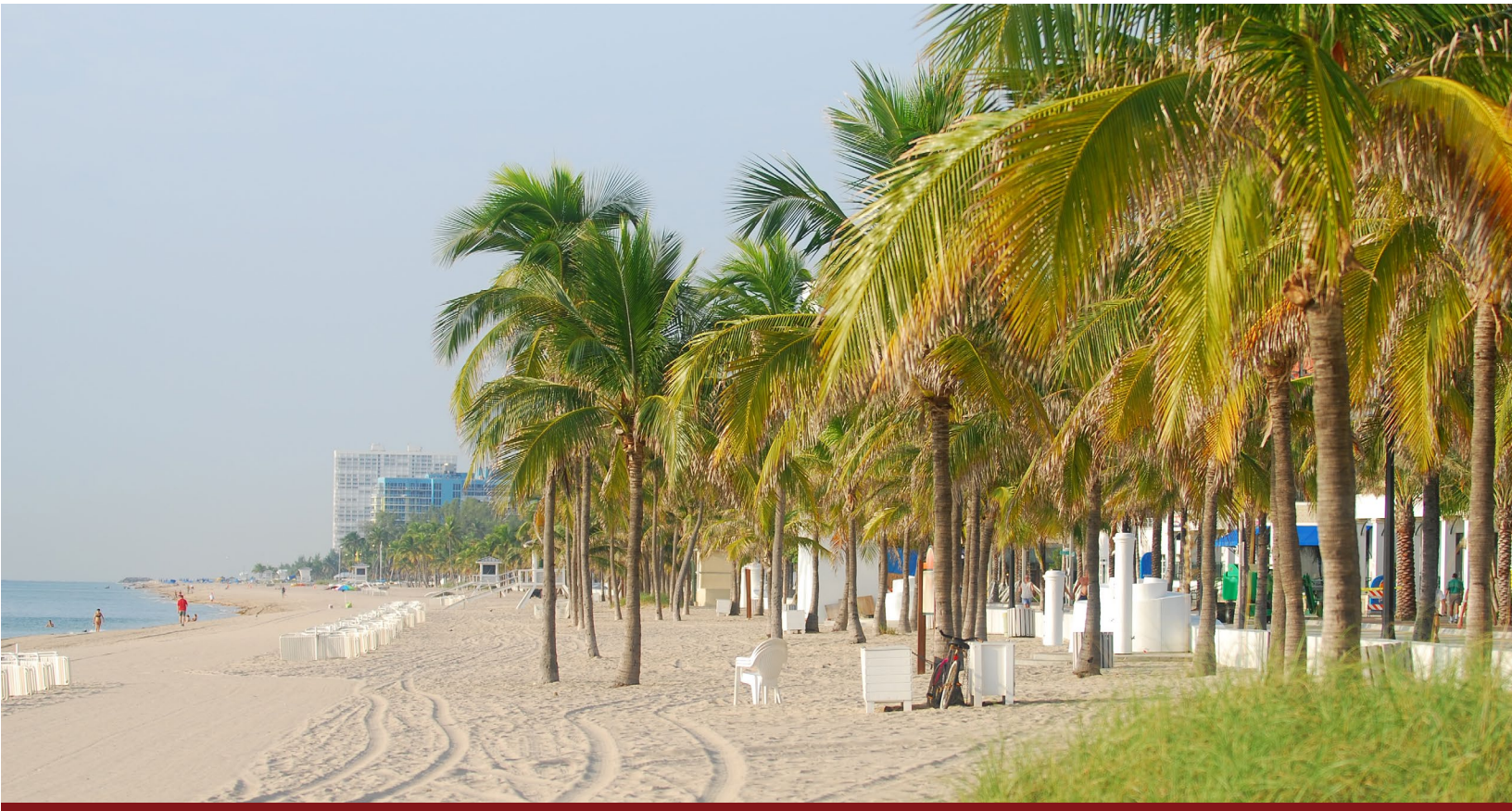
EDI

Upcoming EDI Events:

The 2014 EDI Leadership Summit
October 15-17, 2014 | Fort Lauderdale, FL

The 2015 EDI Leadership Summit
October 14-16, 2015 | New Orleans, LA

This publication is part of a series of Proceedings published by the Electronic Discovery Institute



Adapted from a presentation at the 2012 EDI Leadership Summit
Ft. Lauderdale, Florida | October 2012

About the Electronic Discovery Institute

The Electronic Discovery Institute is a 501(c)(3) non-profit organization dedicated to resolving electronic discovery challenges by conducting studies of litigation processes that incorporate modern technologies. The explosion in volume of electronically stored information and the complexity of its discovery overwhelms the litigation process and the justice system. Technology and efficient processes can ease the impact of electronic discovery.

The Institute operates under the guidance of an independent Board of Diplomats comprised of judges, lawyers and technical experts. The Institute's studies will measure the relative merits of new discovery technologies and methods. The results of the Institute's studies will be shared with the public, free of charge. In order to obtain our free publications, you must create a free login with a legitimate user profile. We do not sell your information. Please visit our sponsors - as they provide altruistic support to our organization.

All EDI publications are free and available on the EDI website at www.eDiscoveryInstitute.org