Zen & The Art of Legal Networking

INSIGHTS & COMMENTARY ON RELATIONSHIP BUILDING WITHIN THE INTERNATIONAL LAWYERS NETWORK

PUBLISHED BY

Lindsay Griffiths

Zen & The Art of Legal Networking

Posted at 7:33 AM on November 8, 2010 by Lindsay Griffiths

Conference Review: ALM's Social Media: Risks & Rewards - Privacy and Security in Social Media

The second session of ALM's Social Media: Risks & Rewards also focused on the risks of social media. Orrie Dinstein, the Chief Privacy Leader and Senior IP Counsel for GE Capital spoke on Privacy and Security in Social Media.

He started by saying that there had been a global conference of data commissioners the previous week in Jerusalem, and the most interesting thing about the conference had been its theme - a new generation (of users, laws and technology), which all converges in the social media space.

It was clear from the comments at the conference that there's so much interest in the social media space, but no one knows what to do with it and it's constantly evolving.

Dinstein focused on privacy and security in social media - or a lack of privacy and insecurity. He didn't offer any solutions, but instead raised a number of points about this complicated space, beginning with security.

Security

Dinstein said that what we're seeing in security is a variety of things. He commented that people didn't used to know that Facebook has over 500 million users when he would poll the audience, but now everyone does. If it were a country, it would be the third largest in the world. People want to be on Facebook, so that's also where people can find and steal stuff.

Viruses, spam, targeted attacks against users, organized crime - all of this is happening in social media. Hundreds of Facebook groups are made up of hijackers and the content that you see on a page might not be benign.

Twitter is also a growing security minefield. These are the sites that attackers are targeting, because that's where the users are.

Dinstein gave an example of a scam on Facebook where an Ikea gift card was being offered. 40,000 people had clicked on it before Facebook found out. There was a similar scam for a Whole Foods gift card, which also had tremendous success before they took it down.

Another issue is "scareware" - people get an ad that tells them that their computer is infected, but when they click on it, the software attacks their computer. Dinstein said that if you get a message that something bad is going to happen unless you act, nine times out of ten, it's a fake. These types of attacks used to come in by email, but now they're coming in through social media.

He said that these scams are all over and people are falling for them at an alarming rate. His biggest pet peeve is the physical side - social media has given rise to cyber stalking and burglars using Facebook and Twitter to target people.

Dinstein observed that people feel compelled to tell the world where they are, which also tells people where they're not. He said that a fugitive had been caught because he'd updated his Facebook status with his location. Twitter has added locations, so now people know where you're tweeting from. Facebook has also added geolocation.

The site www.pleaserobme.com had highlighted people who used social media to tell where they were. The site was satisfied with the attention they had gotten, so now instead of outing people, they are inviting them to read their articles and become educated. Dinstein added that one home insurer is considering raising premiums for policy holders who use social media.

In New Hampshire, Facebook was sued because people were burglarized after posting their locations. Dinstein said that social media is fascinating, but when you forget about the security aspect of things, you are assuming your own risk.

Privacy

In terms of privacy, Dinstein said that people will post anything, and expect it to remain private. People may know that Facebook passes on certain information, but there could be four or five other players involved that they don't see.

This goes to the core of what the first session focused on - when you do read a privacy policy, how much do you really consent to?

Dinstein mentioned that people have started to look at the idea of putting privacy policies on a label. He said that we're a long way from that, but it will be interesting to see how it plays out.

He commented that social networks lead personal data, so too much information on social media leads to issues. There are some interesting ways that this data can backfire. Dinstein said there was a project at MIT where the students had a theory. They thought they could decide based on someone's online profile whether they were gay or not. The project had a 90% accuracy rate, including many students who hadn't yet outed themselves.

Dinstein added that there are medical students who are violating privacy, collection agencies who use social media sites to find debtors, the IRS and DOJ using social media to track deadbeats, etc. He talked about the woman who got disability for her depression, but when her insurers saw Facebook photos of her on the beach and drinking beer, they revoked her medical disability. She's now suing them.

He cited another case of a woman who reported a fake sex ad that had been placed on Craigslist, using information that came from her Facebook page.

Dinstein said that when you work in a work environment, there's often the perception that Facebook is not related to work, and if the employee accesses it from home, it's not their employers business. However, they're increasingly seeing people lose their jobs for their online activities.

Losing Your Job When You Complain About Work Online

He commented that it's fairly obvious that something you say outside of work about work can affect, and most people would agree with that. For example, if someone violates confidentiality, insider trading rules, etc. they're not shielded from ramifications just because they do it outside of work.

Dinstein mentioned a couple of examples of this - a police officer resigned about talking about "arresting stupid people" on Facebook. Another sheriff was fired for a bad MySpace profile. A teacher who posted a blog with personal student information was force to resign. A professor was suspended after making a comment about a "hitman" in a post.

A lawyer blogged about a bad case and called the judge an "evil, unfair witch (EUW)." The judge read the blog, filed actions against him for contempt of court and he was fined. The lawyer thought it would be covered under the first amendment, so he appealed it. It went all the way up to the Supreme Court who upheld the sanctions.

Dinstein talked about convict who's seeking a new trial because of the conduct of the prosecutor on Facebook. A judge who went onto a newspaper's site and anonymously made comments about the trial she was presiding over, expressing opinions about the defendant and his guilt. It was found out who she was and she was accused of having a bias. She refused to recuse herself and sued the newspaper for $50,000 because she said her privacy was violated.

An employee of Microsoft walked by a loading dock and saw Apple's G5 computers. He wrote on his blog that even the guys at Microsoft use Apple computers. He lost his job, and then updated his blog to say that it's bad to complain about your employer. A waitress was fired because she complained about a tip on Facebook.

In the medical field, seven doctors and nurses were suspended for playing a photo game at work. Five were fired for discussing patients on their Facebook pages. A hospital worker who met a cop killer who was injured in a fight with police mentioned that he was in her ward on Facebook.

Dinstein added that this is also happening abroad, mentioning a Virgin crew who was suspended, and cases with Vodafone and in Russia.

He also mentioned a new and interesting trend that he's starting to see - someone was sued for non-solicitation based on their LinkedIn account. He said that companies used to be able to protect their salesperson's contacts when they leave a job, but with LinkedIn, it's hard to prevent them from taking their contacts with them. He's seeing lawsuits that say that people are unfairly using their contacts when they switch jobs.

Losing Your Job For Non-Work Comments Made Online

Dinstein then said that he thinks that the things you do and say that are not about work can and should affect you.

He gave several examples of this - a school employee was fired over a Facebook posting that the school didn't like. A bus driver was fired over a comment on Facebook about a story that appeared in the local paper. The school claimed it was for inappropriate conduct, but he said it was because of the posting.

A CNN anchor was fired after a tweet about Hezbollah. Someone was fired for tweeting to the governor after hearing something that she didn't like. An accountant sent a tweet to friends about getting them to "clear up the

weather" or he'd "blog up the airport." The secret service came to his house and arrested him for threats. He was charged and fired, even though he was making a joke.

An employee for a religious not-for-profit had a sex blog, and although she did everything she could to remain anonymous, someone discovered this and she was terminated. The termination letter said that she was held to a different standard, and should keep her affairs private. Although she tried to, once the information made it into her workplace, it was not in line with her mission.

Dinstein mentioned the Labor Relations Act, which applies to non- and union workers. He said that they have political opinions which are protected, but not in the workplace. There are some off-duty rules, but with caveats. Not all states have them and most that do, have a lot of exceptions. He added that outside the US, there are many more stringent rules on privacy on the labor and employment side.

Dinstein commented that if audience members still didn't think it was a big deal, two out of five employers said that they've found content on sites that have made them not hire someone. He said that Google's solution to the use of social media in hiring is to change your names - declare "name bankruptcy." Google suggested that when teens turn 18, they get rid of their "bankrupt name" and come up with a clean slate.

Stephen Colbert took a humorous and intriguing look at this and other social media issues in a video in August.

Company & Employee Privacy

Dinstein said that international privacy laws come into play when you look at social media, if you work there or if you use it. There are questions about data transfers, about notice and consent and he said that the EU and Canada are investigating Facebook about tagging in photos, whether Facebook really deletes cancelled accounts, geolocation and privacy.

He mentioned that a lot of people say that they're not on Facebook, but they don't realize that others can put stuff up about them and tag them in photos, even if they don't have a Facebook profile. Other people can create a whole world of information about you even if you're not on there.

Dinstein said that there is no easy answer, and if you take privacy laws to the extreme, that could be the end of Facebook. Canadian regulators have taken Facebook to task, and he's not sure how far the EU will go.

From a privacy laws perspective, things get interesting. Improper searches, right to privacy, personal emails sent through webmail using a work computer are all issues. If someone uses their corporate computer to send a personal email, and employer can access and read it. In one case where this happened (an employee used her personal email to correspond with her attorney about a case against the company while at work), the company said they had a policy that says there's no expectation of privacy at work, but the court ruled against them. However, it may not be the same if it wasn't a privileged communication.

Dinstein talked about SMS and tweets sent through corporate cell phones - in one case, a police station had an allotment of texts that could be used for business and overages were to be paid if they were personal. A local sergeant told people that if they didn't want their messages to be read to distinguish between personal and private ones, they could just pay the overage.

One person took him up on this, but the messages were read anyway and it was discovered that most of them were not work related, and he was fired. He said it was an invasion of privacy and the court ruled very narrowly, saying that the search was reasonable.

Dinstein talked about monitoring the use of social media sites, because sometimes it might be required. He said that FINRA issued guidance at the beginning of the year about how to deal with brokers' use of social media - there's an obligation to monitor communications.

Social media raises fascinating questions in the workplace, which Dinstein said was a big topic of conversation at the Jerusalem conference. He doesn't really have a good answer, and some of it becomes more complicated when you add in the international dynamic.

He mentioned that colleagues often ask him whether they should even allow employees to have access. It's a question companies should be asking themselves if they haven't done so already. This also raises the question of using a company email for social media sites.

Dinstein added that recommendations and endorsements can also be a tricky area - no one would recommend a coworker who had left the company because of strict regulations. Someone may do so verbally, but they would be concerned with liability. This would be the same for vendors. But on LinkedIn, coworkers start endorsing each other and it can open them up for liability or raise issues at your annual review.

Connecting with coworkers on social media sites also raises some interesting issues - they may not feel that they have the freedom to say no, especially if the person inviting them is more senior. Dinstein also mentioned whether companies can control what their employees say - how much can you tell them what they can and cannot do? It's necessary to reduce it all to clear guidelines that people can read and understand.

Social Media & Hiring

Increasingly, social media is being used to perform background checks. There are certain questions that a potential employer can't ask a candidate, such as whether they're pregnant, how many children they have, etc. But this information is often readily available on social media sites.

Some of it is protected data that you shouldn't have, but you can get it from accessing a person's Facebook page. Some employers go out of their way to access this information, but they don't often take into account false positives or the wrong identity - there is often more than one person with your name. If you have a common name, someone might decide not to take a chance on you based on another person's social media information.

Since someone can make claims against a company who decides not to hire them based on their Facebook page, it's better to check social media in the pre-hire phase. This is when companies do drug testing and check references because they're thinking of hiring you, so companies can get away with a lot more.

Because of this, some might suggest not searching for a potential candidate online at all but Dinstein pointed out that you may find out that they're a bad person. He said that it's interesting to see how much you can and should know about potential hires, but warned against false positives.

He said the biggest challenge is getting employers and managers to understand that we have to move away from the notion that what we do and say at home is personal and has nothing to do with our work life. Not everything is actionable, but a bad impression will follow you, which can bring a whole host of challenges - that was Dinstein's key takeaway.

Dinstein opened it up for audience questions.

Question & Answer

Question: An audience member asked if Dinstein had any comments about Firesheep, the Firefox extension.

Answer: Dinstein said for those who didn't know about it, Firesheep is a new extension on Firefox which recently came to light because it can be used to steal profile information on Facebook. He said it highlights one of the additional risks of social media accounts and that you can't rely on your privacy settings to protect you (for more information about Firesheep, see Peter Shankman's recent post about "Why it's time to say goodbye to free wifi - part 2")

People should assume that when they post things on social media, people that you don't intend to access that site can see your information. He said speaker from Microsoft at the conference he recently attended shared information on how kids use Facebook. He commented that children don't understand privacy, which is why researchers get a skewed answer about whether they care about privacy. They don't understand the settings as they're set up.

Even people who think they understand their settings don't really understand them. To Dinstein, it all goes to the same point he had made earlier - whatever you post online, someone, somewhere can find it. Everything you post - photos, statements, locations - assume that it will be accessed and viewed by someone other than who you really wanted to see it.

Question: An audience member asked how social media screenings are done during the hiring process - do companies have the candidate present, or conduct them when they are not present?

Answer: It depends on the practice of the employer. Dinstein cited a case where someone was forcing new hires to share their Facebook pages with their employer. He said that some colleges do this during the interview process as well. Kids are starting to create college admissions Facebook pages.

He said that there's no right way, but he suggested a timeline that presents fewer risks. It's important to show that the company has a policy, but they don't want to discriminate. Also, if social media sites are the reason for not hiring someone, Dinstein said it's important to retain that information so that they can show why they didn't hire the person.

Question: From GE's perspective, do they have any best practices to share in terms of what would be good in a social media policy for employess?

Answer: Dinstein didn't talk about their actual policy, but mentioned some of the things he had alluded to earlier. The most important thing is readability - if it looks like your privacy policy online, then you've failed your mission. He suggested making it as short as you can get away with.

You could reduce it to "don't be a moron," but since this may mean different things to different people, companies should have a few articulated rules that are easy to understand and follow. No legalese. He said that a rule that runs more than three to four lines is too long.

Dinstein also recommended recognizing who the audience is - employees. But it may become people who sue the company and say it's a violation. It might be a regulator. The public, if the policy if public.

Question: How easy is it for a Facebook user to know who has viewed their information?

Answer: Not easy at all. There are three parts:

1. Who are the people you have given access to? This depends on your privacy settings.

2. Who are the people who are surreptitiously accessing your information? Crooks, college administrators, etc.

3. Advertisers: Advertisers can intentionally or unintentionally get information from Facebook.

Dinstein mentioned one instance where Facebook found out that their users IDs were being embedded in a URL. There are applications for who has checked out your profile, but these have nothing to do with Facebook and he hasn't determined yet if they're illegitimate or only partially illegitimate. Dinstein said that when in doubt, it's best not to click, even if you're really curious.

Question: An audience member asked about the medical use of Facebook pages.

Answer. Dinstein said that anecdotally, it's not very common, but to the extent that access does take place, it's more on-the-spot demand. It's not usually with a privacy agreement. He said that the practice is evolving again as companies and colleges become more formal about their policies.

Question: Do potential job candidates have a legal right to say that the company can't access their social media information?

Answer: Absolutely, but the question becomes if you get a refusal of an offer, was it because you refused to share information? If you have nothing to hide, then you shouldn't worry. He said in the past, it used to be easy to be private and took an effort to be public. But now, it's the reverse - public is easy and private is hard. Now you have to work to be anonymous. If you have nothing to hide, then why wouldn't we know everything about you. If you're coming to a job interview and you don't let them see your Facebook page, they will think the worst.

Question: Is it true that if you have your privacy settings set a certain way, there's no way to tell if you're on Facebook?

Answer: Yes, but that kind of defeats the object of Facebook. Dinstein said that in Japan, most users use a pseudonym on Facebook, and if you don't know that, you can't find them. He said that people have mixed emotions - they go on Facebook to become friends with the people they went to kindergarten with, but if they use a pseudonym, it fails.

Question: Is anyone using social media for vehicle financing or skip tracing (to find missing cars)?

Answer: He didn't know if they're doing that, but he knows law enforcement is using social media sites to look for fugitives and debt collectors are using them. He couldn't imagine that people looking for someone wouldn't use all means to do so. As long as you're not behaving illegally, there's nothing inherently wrong with going on a Facebook page, and, if it's public, finding information.

Lindsay Griffiths of the International Lawyers Network
179 Kinderkamack Road
Westwood, NJ 07675
Phone: (201) 594-9985
Fax: (201) 740-9765