ASSOCIATION OF CORPORATE COUNSEL

TITLE: **The Millennial Generation in the Digital Workplace: Emerging Data Security, Privacy, Harassment, and Liability Issues**

DATE: **November 11, 2008**

PRESENTED BY: **ACC Employment & Labor Law Committee**

SPONSORED BY: **Morrision & Foerster**

FACULTY: **Karla J. Elliott**, Vice President, General Counsel and Secretary of Eagle Adjusting Services
Alison M. Gardyne, HR Legal Attorney, Intel Corporation
Daniel P. Westman, Managing Partner, Morrison & Foerster's Northern Virginia office, and Co-Chair of the firm's Employment and Labor Law group and the Trade Secrets group

MODERATOR: **William Harn,** Past Chair, ACC Employment & Labor Law Committee

*****

Operator: Welcome to this ACC webcast. Bill, please go ahead.

William Harn: Good day, everyone. My name is William Harn. I am the Immediate Past Chair for the ACC Employment and Labor Law Committee. It's my pleasure to welcome everyone to this webcast entitled, The Millennial Generation in the Digital Workplace: Emerging Data Security, Privacy, Harassment and Liability Issues.

Just a bit of housekeeping, I wanted to let remind you that this is – webcast is being sponsored by the IT and eCommerce Committee of ACC as well as the Employment and Labor Law Committee, and the Southern California Chapter, also known as ACCA-SoCal.

Information about the Association of Corporate Counsel and/or – either of these committees can be obtained by going to the ACC Web site at, www.acc.com. I would encourage anybody on this call who is not a member of the committee to join a committee and become actively involved.

The IT and eCommerce Committee meets on first Thursday's of every month at noon. Information for the dial-in teleconference is available on the www.acc.com Web site. And the Employment and Labor Law Committee meets the first Wednesday of every month. Their dial-in information is available at the same Web site as well.

A few housekeeping issues for you to know. If you notice on the left hand-side of your screen, there are two boxes. One is entitled links and one has a box where you can enter the lower left corner of your screen is a box where you can enter questions if you may have them during the course of today's webcast.

In the links box, you'll please note item number six, it indicates seminar evaluation. When the seminar is completed, if you would do us a big favor, we need your input and evaluation as to

how you think the materials were presented, substantive matters if were covered adequately and if there are anything – if there is anything that any of the presenter can do in making these webcasts a further success for you in the future.

Again, if you wish to ask a question, just type your question into the lower left hand box. We'll field the questions if they are appropriate during the course of the webcast. We will ask them up to speakers as we move forward, otherwise there will be quick Q&A session towards the end of our presentation.

Our speakers today are an esteemed panel of individuals who have a wealth of employment and labor law experience as well as experience with eCommerce and electronic privacy issues.

Karla J. Elliott, Vice President, General Counsel and Secretary of Eagle Adjusting Services is our first panelist. Ms. Elliott has counseled and litigated on behalf of public and private companies, as well as governmental or in quasi-governmental entities, as a labor and employment litigation attorney with law firms in Washington, D.C. and Indianapolis.

As I indicated, she currently serves as Vice President, General Counsel, and corporate Secretary for Eagle Adjusting Services, a premiere property and casualty independent adjusting company. In addition to those responsibilities, she is also responsible for all Human Resources, Corporate Education, and Information Technology functions at Eagle.

Ms. Elliott received her J.D. cum laude from The John Marshall Law School in Chicago, Illinois.

Our second panelist Alison M. Gardyne is an HR Legal Attorney with Intel Corporation. Over the past 15 years, Alison has focused her practice upon employment counseling and litigation for a wide range of public and private technology companies in Silicon Valley. She is an HR Legal Attorney for Intel, the world's largest semiconductor company with over 80,000 employees worldwide.

Prior to joining Intel, Alison spent five years managing the global employment law function for Yahoo! Incorporated, a leading Internet company. Ms. Gardyne has also had the benefit of knowing what it's like to be a client prior to joining – attending law school, she was a Human Resources professional for several years. Ms. Gardyne received her J.D. from Northeastern University School of Law in 1993.

Lastly and but not least, our lead panelist today is Daniel P. Westman. Daniel is a managing partner of Morrison & Foerster's Northern Virginia office, and Co-Chair of the firm's Employment and Labor Law group and the Trade Secrets group. Mr. Westman has represented management in employment, trade secret, employee mobility, and computer fraud litigation and counseling matters since 1982.

Mr. Westman is also the lead author of the book “Whistleblowing: The Law of Retaliatory Discharge”, the Second Edition, which is published by BNA. This book focuses on the whistleblower provisions of the Sarbanes-Oxley Act of 2002, and has been cited in opinions of the U.S. Supreme Court and the Supreme Courts of six states.

Mr. Westman obtained his law degree from the University of Chicago Law School in 1981, and has previously served as a law clerk to Honorable Barbara Crabb, U.S. District Judge, Western District of Wisconsin.

I could list all the course where he is admitted, but I think the only place he is not – that he is not been admitted is Western district of Marianas Islands.

What I'd like to read into this presentation for our panelist is that this presentation is going to focus on a lot of issues with respect to the Millennial Generation. And one of Mr. Westman's

specialties is dealing with the tension between confidentiality and disclosure. And he has brought into sharp focus by it's into relationship – that interrelationship with the Millennial Generation and its use of technology.

Mr. Westman comes with a great deal of experience in this regard with he and his wife have three teenage sons who teach him daily about Millennial working styles. Dan?

Daniel Westman: Bill, thank you very much and thank you to Karla and Alison and you Bill for joining us. Our agenda today will be a few brief remarks about the electronic workplace that most of us work and irrespective of what industry we are in. Then we will move into the brief discussion of the four generations in the workplace today.

And then spend most of our time talking about how the millennials' have what I refer to as a 24/7 connected lifestyle and how they are bringing that lifestyle into the workplace. And we will end up with everyone's topic emerging employer exposures resulting from the millennials' coming into the workplace.

So, there was an indictment unsealed in April of this year in Chicago, which illustrates I think the commercial problem, we all face very well. Hanjuan Jin work for Motorola and she was arrested at O'Hare airport on February 28th, 2007 with a one-way ticket to Beijing.

In her possession where what Motorola said were about $600 million worth of trade secrets contained on laptop, four external hard drives, 29 recordable discs, the thumb drive and the good old fashioned paper documents.

She had been on a leave of absence came back from the leave on February 26 and 27 and in that short period of time copied all those materials and was at O'Hare ready to go to China.

So a few reflections, what does that tell us about the electronic workplace people and data move around the globe very quickly today. Secondly, 10, 15, 20 years ago most companies probably stored their most valuable data under lock and key, in a safe, with a combination lock on it. But now there is lots of confidential data is stored on computer networks, wide access is given to employees to those networks and it's very easily copied and removed.

Another reflection about this Ms. Jin had a laptop and four hard drives, what used to be a very expensive corporate or institutional purchase namely 250 gigabytes of storage. 20 years ago, only the largest entities could afford that. Today, it's a $100 at your local electronic store.

So, what used to be incredibly expensive devices or storage devices are now consumer items that anybody can buy and bring it to the workplace and in fact that's happening. People are bringing their personal devices into the workplace using them for work purposes and not necessarily telling their employer that's what they are doing.

So at the end of every trade secrete litigation, we handle or data security breach that we handle the client always asks, how can, we avoid this because we never want to repeat it again. And our answer always is, you need to have an effective data security program, and what that means, is you need to know how people are using your technology.

So, let's move on to a brief discussion of the generations and how the different generations probably differ and their use of technology. There is a lot of generational literature out there and I don't pretend to be an expert on this. There are people, who do. But this is a summary of the literature.

And what the literature says is that people are living longer, retiring later and this is the fulltime, first time that four generations are working in the United States in a workplace together.

They are – what we call the Mature or Worldwide II Generation; the Boomers typically born in the 50s and 60s; Generation X after the Boomers and the Millennials or Generation Y definitions differ, but typically people born about 1980 or later, who grew up with the technology that we all have now and the Internet is an integral part of their lives.

And what's fascinating about this literature is it suggests that each generation has different values and beliefs as a result of their experiences growing up.

This pie chart tells the demographic story namely. Today, about five percent of the workplace is Mature Generation, 45 percent are Boomers, 40 percent Generation X, 10 percent Generation Y. But what we know as just a fact of life is that lines on this pie chart will be moving counter clockwise.

The number of Generation Y/Millennials will only increase overtime and we'll talk about this a little later. Generation Y or young employees will probably be supervising older employees. There are 70 million Generation Y/Millennials. They are by far the largest generation now and it is the fastest growing segment of the workforce. So, if you're not seeing this in your company yet, you will be seeing it very soon as the millennials come into your workforce.

Alison Gardyne: Dan, this is Alison. I would just wanted to comment from – I think this pie chart is a good representation of the workforce in America as a whole. But you certainly will find differences sort of dial-in although depending on where you are certainly in Silicon Valley and especially some of the startups, this picture would look very different.

So, the 10 percent is going to be much higher and they're rather going to be much bigger in terms of a much younger workforce, where oftentimes the average age of employees at companies is in the early 30s. And so, I would imagine that you can have (other flip side) to other more mature industries where there are going to be differences as well.

Daniel Westman: At some point every company is different to be sure different generational composition. Briefly the Mature Generation is people born before 1945, the defining events in their lives. While Worldwide II, the depression either they experienced or their parents did in the rise of labor unions, which were new in the 1930s.

As a result, their values tend to be respectful of authority. They came of following the president in through a war. They are loyal to their country and company. They are proud of conforming, standing out or blogging, which they never heard of until recently, is not necessarily a good thing. They believe that if you are at the top of the leadership pyramid, that you got the perfect reason and they are willing to make sacrifices for the greater good.

The boomer generation typically is viewed as having grown up with Vietnam; in civil rights era, assassinations of civil right leaders and political leaders; the cold war; and television was the new technology, if you can believe that.

But in terms of values, their president was Nixon, who was impeached or about to be impeached. So, there is love/hate relationship with authority; tend to be pretty driven, hard working, and if they work hard they want more money; they believe in leadership by consensus, if you are at the top of the pyramid, you didn't necessarily get there by merit; they would like to fit in if possible; are interested in material things to display success; and sacrifice for them is working hard to achieve.

What's interesting about the generation of literature is, it notes that the media and, not just the media, but people do recognize membership in a generation, although each of us is different and not all of us share all of this characteristics of a particular generation. There is recognition of differences between generations. And for example, in 1967, TIME magazine fostered that generational recognition by naming as Man of the Year, the Boomers. So, there is a little bit of generational rivalry all the time.

Generation X is the post boomers. Defining events for them are Watergates; Latchkey kids two career couples and day care; dominating in their lifetimes AIDS came around; the new technology was MTV and cable TV.

They tend to be not terribly impress the authority; have a work ethic, but they want to have a work like balance; they believe in leadership by competence, so being at the top hierarchy if you doesn't necessarily mean anything to them; they saw events in the world affecting their families; and they will work hard, but you have to show them why they should work hard; they will fend for themselves, interfere themselves when the folks were at home; and sacrifice for them is forfeiting personal time.

Millennials/Generation Y grow up with the Internet corporate scandals, Enron, WorldCom were the headlines in their youths, Columbine and 9/11. So violent acts against high school kids and against our country were part of something they grew up with. And that point was driven on to me little while ago when our youngest son said, "We had the DC snipers here for several who were causing a lot of anxiety." And as I was putting him to bed one night, he said, "Dad, did they really get the snipers?"

So, it's – as personal security is not given for this generation. They are relaxed about authority. They are ambitious. They believe in leadership by achievement. They want to stay connected all the time, if anybody has child or acquaints, who walks in the door and gets on Facebook right away, you'll know exactly what I mean or who is always texting, rhyming. And they lead a busy life; they want to have work; they want to have personal life; and they want it to be in balance.

So, let me stop there and ask if any of our panelists have reflections about the generations before I move into how the different values can affect the workplace.

Hearing nothing, I'll move right ahead. Millennial's more or so than any other generation used technology fluently and stay connected with each other, whether it's through cell through IMing, through texting, or Facebook or other Mechanisms. And that has led to what the literature describes as different values and styles in many different ways, for example, communication etiquette.

There was a millennial who wrote into an advice columnist and said, "Is it OK, if I am running late to a meeting to IM my boss and say I am running late." And the columnist wrote back and said, "If your boss is older than you know the boss will think you are hiding behind the technology. You should call, apologize like an adult and be polite." So it's not a given that millennial will necessarily share the same view of what communication is appropriate in every circumstance. Blogging, another perfect example of that.

Boundaries between "Personal Timing" and "Working Time." Technology makes it possible for almost everybody to work at any given time from many different locations if they have a secured network to get into their company to work on. So, a millennial may not think twice about sitting at their computer, watching YouTube during the working day, whereas somebody of an older generation might view that as stealing time from the company or stealing bandwidth from the company that the person should be using the time in the office to interact with colleagues. After all that's why everybody is there during the work day.

Privacy is a significant issue. People will put things on blogs or on Facebook or on MySpace that are kind of hard to imagine for the people of other generations, will talk at great length in a moment about personal versus corporate use of technology, big differences there.

IP ownership. This is the generation that grew up swapping software, swapping videos, swapping music, saw Grafter's business model go up to the Supreme Court. And even though it was invalidated, probably we thought we won that battle because now we have iTunes and we

don't have to buy the whole CD or the whole whatever, we can just buy a single song. So even though we lost the liquor war, we won the battle and by changing of how the business of music is operated.

Millennials probably more saw than any generation before have seen their parents or people older than them switching jobs whereas somebody of my – I am a baby boomer or my father worked in a single institution in its entire career.

It's unlikely that many millennials will have that experience and that will have an effect on their view of whether it's appropriate to move from job to job and what kind of institutional loyalty they have. So as you can see almost any issue that you want to identify millennials probably have a different view than older employees.

Karla Elliott: Dan, this is Karla. I think one of the things that it's interesting to point out too and we're talking about these values and beliefs affecting how the millennials are working within the workplace. It's important to keep in mind too that these things also affect how they interact with our customers and clients.

So we have – we all have very different views on what maybe appropriate for communications within the workplace, but that extends out to the people that we're dealing within our businesses as well. So, a lot of the things we're talking about here apply to that relationship too.

Daniel Westman: That's fascinating point. We've got some software clients, who effectively have chat boards for their clients. So, these very technology-savvy customers, who want to interact via e-mail and the chat board with our client and will be perfectly happy and they will just speak to a customer, which maybe anathema to – in other companies, which price that personal interaction with customers and that's a great point.

OK. Symantec, which is a security firm in Silicon Valley, came out with the report this March. I don't know how much publicity it's gotten, but it should get a lot. It highlights how millennials view the use of technology and it's a little bit scary.

So 69 percent of millennials say they will use whatever application technology or device they want regardless of its source or corporate IT policy and I'll say something here that I'll repeat later that 69 percent of the people who admitted it. There could be some of that 31 percent they are just are not admitting it. In contrast, the older generations say, most of them say, we'll follow the policy.

A 45 percent of millennials say they'll stick to company issued devices over two-thirds of the rest of us say that we won't. Three quarters of the millennials say they've downloaded software at work for personal use and one quarter of the rest.

Continuing 66 percent of the millennials admit to regularly accessing Facebook and MySpace. I think that number is higher. The rest of us 13 percent accessing Web mail account, 75 percent of the millennials, 54 percent of the rest using IM over the corporate network, half the millennials, quarter of the rest.

Let me dwell in Web mail for a moment with a lot of ISPs now offering storage along with their Web mail accounts, it is possible for an employee to upload documents to the storage provided by the e-mail.

So, the documents will be sitting on the server of ISP not on the company server and could be downloaded from other places. Unless, the company has in place the policies or screens to prevent that from happening. So, accessing Web mail may sound benign, but with the storage that's available through those accounts now, it may not be benign. We are seeing some cases involving that.

Alison Gardyne: Hey, Dan, this is Alison. I think on this chart too the IM user bit again really depends on the corporate culture and there are plenty of companies, where IM is the way you do communication and (it's not) possible IM screens going on at one time.

And so I think that in those companies, where that culture is prevalent, the number of others where you have only 22 percent on this chart using that I think that would be vastly higher. It will spread across the culture of the company, if you have a predominantly technology driven culture within your organizations.

Daniel Westman: Alison in your experience, are the IMs captured on the company's server, does it run over a company server or does it running over something else so that the company can reconstruct it if they need to?

Alison Gardyne: It really depends I mean at Yahoo! Obviously, it's Yahoo!'s IM. So it is a – there was always a tension there between the corporate use of IMs even though it was on the company's product. So anybody can use Yahoo!'s IM and when employees did it, we had special issues there.

IM is used at Intel (rhyme) at the moment and it is a Microsoft's product and so those are captured and hosted on our own site. So that it really depends how you setup and enable the IM piece of that.

Daniel Westman: The reason I've had as we've had such harassment cases that were conducted over IM. We've had trade secret misappropriation done via IM and we've had one company had a drug ring, where the employees used IM to coordinate their pickups and drop offs of the products.

Alison Gardyne: Absolutely and it looks like one of our participants made a comment here that internal IM can cause great distress. It's needed for e-discovery and AIM in for that is all I can say that is absolutely the case. And if your company does have IM and use that first of all it's a treasure throw of information, you would be amazed that where how much harassment will take place on an IM.

But it is something that absolutely have to get your hands around and make sure that you know how it's stored, how it's backed up, how you deal with it and you will absolutely need it as part of a discovery process.

Daniel Westman: Excellent point.

William Harn: And at the same time as much as you store this information, you have to be very careful, how you re-access it and who is storing it for you given some of the new case were out there and the – Dan, you may know the exact name, I think is Stored Communications Act. So, how you monitor IM activity can also become very critical.

Alison Gardyne: Yes. And there are some recent cases on dealing with pagers. Information on pagers too and whether it's served on or stored on pager, so the pager company server versus your own company server. That's another thing to be aware of in how that gets handle.

I think a lot of the pager companies nowadays are not turning information over, whereas in the past, without the actual users permission and in the past that would be something that companies could routinely get access to as part of investigations into wrong doing and that type of stuff.

Daniel Westman: Excellent points. Moving along, this is generation that bandwidth is given. So, the millennials, they think nothing about watching, streaming videos over the company computers about photo sharing, about using iTunes and so on. Whereas older people probably can

remember a time, when if you sent to larger attachment on an e-mail, you could crash your e-mail system, or the persons who you send it to, but bandwidth is just given that they've grown up with.

Also troubling from a corporate perspective is the use of personal devices versus corporate devices. Millennials, 39 percent of them say that they will store corporate data on a personal PC; 38 percent say they will do so on a USB drive; and 13 percent on smartphone, don't forget that smartphones with iPods and rest can store data, they are not just simply music tools.

This can come into play in e-discovery in a big way. So, for example, if your company allows people to take data from a work computer, download it on to a personal device, take it home, work on a personal computer at home, doing work perhaps logging into a secure network to do the work, when litigation happens the corporation may feel compelled under e-discovery rules to ask the employees for copies of the USB that they used to take work from the workplace to home.

Copies of the hard drive of their personal computer, so they can see what work was done on a personal computer, and there are few people who want to turn over their personal devices or their personal computers for forensic imaging to anyone, not alone their employer. And I think this is coming up with more and more frequency in our litigation matters (and into) enormous headache.

Alison Gardyne: Dan, I think this is Alison, one other quick point on the phone. It's very hard to find a cell phone nowadays without a camera on it and its there in everybody's pocket. And that's something that companies need to be aware of in terms of access into manufacturing facilities and other places where it is not difficult for anybody that's to pull it out of their pocket, quick snap a picture and that's something that companies need to be thoughtful and mindful of its phone.

Daniel Westman: Well, that's a great point. I am glad you mentioned. You may be asking yourself why is Dan in Northern Virginia on this call. Well, I think it's because lot of our clients are government contractors, who is client themselves, government agencies, intelligence agencies or Department of Defense push security out to the government contractors.

So most of our government contract clients will have literally a secure briefing room with the combination lock on it, and outside that secure briefing room will be a wall of lockers, where employees are required to check all devices, check their phones, check they Blackberries, check anything that could record any data. And other – they are not allowed into the rooms with those.

So, in the Northern Virginia, we see companies that go to the extreme of having no storage on the desktop. They will have a screen. They will have a keyboard, but no data storage. And it's all sitting on a server some place and a no pen and paper rule. So that people can't even copy down what it might be secret from the screen. That's the extreme of course.

Then we have commercial clients who tend to fall into two categories. Those who have been burned by a trade secret case or a data breach who very much appreciate the need for data security that we're talking about here, and those who have not yet been burned and who need to be paying a lot more attention to these issues than we should.

So, absolutely, also in there – it's depending on the nature of the company. A company – commercial entity may want to adopt some of what is common place in the government contracting world depending on the value of the secrets that are flooding around in their workplaces.

OK. Another issue is the concept of privacy. You've probably seen things on Facebook and MySpace that are astonishing to you if you are older, but taking it for granted by the people who use those things. If you've ever opened a Facebook account and I recommend the experience to you if you haven't. You have to read the terms of use – and the terms of use, you are supposed to read them. And the terms of use say that these social networking sites after all are social and they prohibit commercial activities.

So if you are a teen or a young adult using this, you may have an expectation that companies are reading those terms of use and the companies may think, Oh, OK we can't use the information here for our background checking purposes. Well, the terms of use don't say that, but the prohibition of commercial use may create that expectation in the minds of the people using these services.

Also, if you set up an account, you have the ability to control who sees what portion of your page. So if you have a photo section you can limit the photos to just your friends, people whose friend request you will accept it or it could be viewable to anybody, who has access to Facebook.

So these privacy features may create a bit of a false expectation on the part of the people using them that the material posted on the Internet is unavailable and we've learned from our clients that if you know what you're doing you can find your way to these places on the Facebook or MySpace pages that are supposed to be private but actually can be looked into.

So, there is – well others make the comment that in observing our teenagers, they get really upset when you do two things. Number one, when you go into the basement and they are watching a movie with their girlfriend, they don't like you being there even though you have every legal right in the world to being there. And they don't like it when you look at their Facebook or MySpace page because it's a same feeling of intrusion on their privacy.

Alison Gardyne: Dan, this is Alison. Can I just start with sort of – the flipside to that is what most companies and employers would think as private which would be somebody getting disciplined or somebody being laid off in the process of that typically is not something that we think are within the public domain.

And that's not at all how these types of activities tend to be viewed given all the technology. And so, it has certainly been my experience that when dealing with layoff situations and/or just individual managers disciplining employees that can end up being blogged about.

Many companies have experienced sort of live bloggings of their layoff. So people on Twitter or on various blog sites, typing in OK HR is coming to meet with me now, oops I got the package, I only got this amount.

And is that the York Times had an article just a couple of days ago, where they were essentially talking about the phenomenon and saying the companies you need to get out like yourself and blog about it to set the record straight.

Because what you'll get if somebody, who is disgruntled and not happy about being laid-off, who is sort of spreading information out there about the process and you are far better off, if you get out in front of it with kind of a generic statement about it's a difficult day for us et cetera, et cetera.

I think it's something that many companies, you don't need to think about, but you need to so that you don't end up with your communications to employees being out there on Web sites are being copied.

And there is a lot of that, that I think the older generations do not – I would never in a million years post my resignation notice on a public Web site, but people do in the younger generation.

Karla Elliott: Dan, this is Karla. Just a couple of points one to follow-up on Alison's point just now. It's absolutely true that we've got a different view of what could be considered private when you are talking about these types of bloggings and what have you, A, something to keep in mind is regarding privacy issues with the employees putting this kind of stuff out there.

Although we don't have much of a legal issue here in the U.S., where the laws are more protective of our customers or third-parties on the protected and private information on these types of sites. Keep in mind that in Europe of example, data protection laws cover employees and customers equally.

So anything that might be sensitive information that an employee could put out there potentially the employer could be on the hook for liability over a hot-button item like race, religion or what have you. And so that's something to keep in mind when we are talking about the employees just putting anything out there that they want.

Switching gears for a second, going back to the social networking sites. I think it's important here to note too that although some of these social networking sites do prohibit the commercial used site we've talked about many don't. And in fact some even encourage it.

For example, we know that there are several HR Managers from ACC member companies that have noted that LinkedIn is one of their primary tools for finding and researching job candidates now.

In fact social networking technology seems to be so pervasive in the U.S. that I had a fellow committee member shoot me a note this morning that the U.S. Air Force is using social networking technology to foster innovation in the identification and development of game changing and disrupted technologies and the like.

I think the key here is that we can only expect this to increase. When you see people in companies like Marc Andreessen, I believe I'm saying that right. The founder of Netscape, Loudcloud ((inaudible)) other Internet technologies, who is now focused on creating do-it-yourself social networking.

So we're familiar with Facebook and MySpace and LinkedIn. But now there is – even companies out there that are creating a DIY environment where anybody can get on and do it to the hosts content.

Daniel Westman: Those were excellent points. One of our attendees commented that their company blocks access to YouTube, Facebook, MySpace, while at work but not general Internet access. A lot of the government contractors around here do that as well and they are concerned that foreign agents – people in Eastern Europe block or wherever maybe trolling the social networking sites for data.

Karla Elliott: Exactly.

Daniel Westman: And they don't want to have their people out in putting information out there. It's not – it doesn't think you had a recruiting disadvantage in the government contracting space here because everybody expects that.

However, it may in the commercial world as you are attempting to recruit millennials put you had a little bit of disadvantage if they are expecting that. So, that's one intention we're hearing about is how do you do the best job at recruiting millennials sometimes its offering them access to these technology. So, it's a very difficult issue.

OK. So, let me try to put all this together on a data security point. Obviously, if people are – if the reports are at kind of tip of the iceberg that we're beginning to see now about how millennials are using technology is bringing their personal technology into the workplace without necessarily getting permission or telling anybody, using it, and then losing it. I can tell you that some of these data security breaches come about when people lose a laptop or a pen drive or a hard drive, or a phone, with data on it.

You have to have an effective data security program to avoid these breaches and to avoid trade secret cases. And you cannot have an effective program unless you know what your people are doing. You can't have an effective program unless you know are people bringing personal devices into the workplace. How are they using them?

So, one of the literature is starting to develop on this, that some of the most frequent causes of data security breaches or trade secret cases are off network use of technology at home or on travel, where personal devices are being used for work purposes.

So, I am not saying that every company most absolutely prohibit people from using their personal devices, but what I am saying is you need to know that they are doing it. And you need to have a – be able to react and plan for it. We have a lot of clients with very valuable scientific data, who do have per se rules, saying you may not use any of your personal technology in our workplace. If you need you pen drive to take a speech off or a presentation at someplace, you will use our pen drive and it will be encrypted.

So, we know that if you lose it, we don't have anything to worry about. Not every company has go to that extreme, but it is something that has – we see more and more of the data security breaches and trade secret issues may become more prevalent.

Obviously, I am a little bit concerned that the Millennial Generation may not share the same values as to who owns intellectual property. File swapping, swapping movies and so on may not, maybe somewhat inconsistent with the idea that data belongs to the company that created it.

Don't also forget that there is this species of personally identifiable information that is now very valuable in the form of names, addresses, social security numbers that can be use for identity draft. And companies need to realize that they have that information not only about their employees but maybe about customers and other third parties who have (gambit) to them and you need to protect that both from external threats and internal threats. And you need to do an inventory of the kind of valuable data that you have, that is now valuable spices of data whereas 15, 20 years ago it was not.

One hole that we see frequently with data breaches and trade secret cases is document retention on the back-end. That is when you dispose the electronic data, there are instances where companies old cell phones or laptops or Thunder Eyes maybe auctioned on eBay, or otherwise put out in the world. And they may not have been white clean were very easy software to use of company data and that is unfortunately relatively common occurrence.

So, if you have a Record Retention Policy, it's worth looking at the disposable feature of it and leaving in provision that when you dispose off electronic data, you have to check with your IT Department to make sure that its disposed off in a correct way.

And last but not least, it may be obvious but let me state it anyway, if you – if it is true that millennials were coming into the workplace with different mind sets about IT, about who – whether its property use personal technology, you need to train them to your expectations. So if it's worth spending an hour or two in the first week of employment, training against the risk of harassment and discrimination, then, I would suggest to you, it is worth at least that time training against the data security risks.

Alison Gardyne: Dan, this is Alison. I just want to jump in with a quick comment to especially on the personally identifiable data protection. It's really important that you – your vendors are on board and your purchasing department of whoever is engaging vendors is very aware of these issues. Because the same circumstances occur in their workplace and it's not hard to have your EXPAT records and all of that type of stuff on a pen drive that's lost or other circumstances, where information about your employee is being improperly used due to data breaches because of vendors. And so that's another important piece of this.

Karla Elliott: This is Karla to Alison. I think you are absolutely on point there. Taking that just one step further, I think we also need to be mindful when we are dealing both with our internal policies and when you are talking to vendors and suppliers externally, that we're not only looking at the Records Retentions Policies and such that we have set up for our companies. But we also, many of us also have obligations under federal and state laws that are directing these things now too.

You are seeing the increase in ((inaudible)) and all the effects it has. We have been dealing with Cipla for years and yet to find anybody who completely understands that one. So those are all things that come into play as well. When we…

Daniel Westman: I am sorry. Go ahead, Karla.

Karla Elliott: That was it on that point. I was going to move on.

Daniel Westman: OK. Well, I just wanted to – when you look at this list on page 18, it drives home that you need every function in the company working together to solve these issues. So there is an IT function here obviously devices in the workplace uses the computer network. There is an IP function here (patented) or other people are going to want to have and say and what happened.

There is the personal identifiable data issue, which can beg customer issues. So your marketing and sales people, well, let me, you want to have a say in this records retention, nobody knows where that falls in the corporate scheme of things and then training obviously is an HR issue.

So the only way in our view to have an effective data security program is to deal with it as a team to have buy-in input from all the functions in your organization that need to have input and getting buy-in from every function.

It's very helpful to have the tones out at the top if you can get the CEO's attention on this issue. If you can get the CEO to do an introduction in the employee orientation that emphasizes data security. At the same time, is it emphasizes policies against discrimination and harassment so much the better.

But we see – the problem that we see when we were asked to diagnose, how the problems happened is the silo approach either it was just the law department who did it or just the IT or just HR and it wasn't the team event. So strongly urge the team approach to data security.

Karla Elliott: Dan this is Karla again, I think, you are absolutely right there that, that just emphasizes what we have talked about very briefly already. When we are talking about e-discovery without that sort of global approach so that everybody has a piece of responsibility for this.

When you are in the legal department and get a request for something with e-discovery, we may not even know where to begin looking, when we're talking about documents and data that we're trying to recover.

It's not just the corporate server or e-mail accounts. We're talking about cellphones, BlackBerries, PDAs, pocket PCs, thumb drives, instant messaging. It runs the gamma and without all of the pieces of the company working together to manage that effectively. You never know what things are going to be found in which of these little storage areas.

Daniel Westman: Well, and it's a critical point in this era of e-discovery because if you don't find it amongst your employees and your advisory does find it in litigation you are at risk of a court drawing an adverse inference that you tried to hide it. So if you don't go looking for it in the first instance, it's a real problem. I agree with that entirely. OK

So, let's move onto some of the tips of the icebergs that we think we are seeing. When you look at all these issues in isolation, they are kind of – you look at them and you say, while that's an interesting arcane point. I'll just file that away.

But when you look at them in combination, my hypothesis is, what we are seeing is the 24/7 Connected Lifestyle come into the workplace and all of these issues are the iceberg underneath the surface of that Lifestyle coming into the workplace. So this emerging employer exposure is how employers can be bitten by these things.

Harassment in cyberspace used to be kind of a law review arcane discussion, but it was made real by a case out of New Jersey, where somebody named Blakey took offense at some comments made by a co-worker about Blakey on a bulletin board that wasn't even sponsored by Continental Airlines, it was sponsored by the employees.

Yet the employees brought those offensive materials to the attention of Continental and Continental didn't do anything about it and the New Jersey Supreme Court said that is a sufficient basis for harassment claim.

Once the company was unnoticed of the harassment, the company had an obligation to try to do something to prevent it from happening again, so allow that lawsuit to go forward.

Blogging, Ms. Simonetti for some reason these cased come up in the airlines industry, I don't know why? Ms. Simonetti posted a photo on a Web site, I don't know if it was MySpace or Facebook but on some Web site of her in her Delta uniform which had kind of open blouse and kind of a shortcut skirt and she was sitting on the back of one of the seats on the plane in a fashion that Delta found too risky and they fired her.

And she filed a lawsuit saying well that's differential treatment because you didn't fire the Male steward, who said on his Web site that he likes to watch pornography and that's far more offensive than my photo wearing my uniform and that case was put on hold by the Delta bankruptcy.

But it was it got passed got into the court house and passed a motion to dismiss and is an example that if you're going to discipline employees for blogging, which is coming up with more and more frequency, be careful and be consistent and avoid situations, where you're only disciplining the women or the older or younger or whatever the protected category is.

There is Whistleblower protection for some blogging. There is (provision) of the National Labor Relations Act that protects what's called protected concerted activity that is employees talking to each other about dissatisfaction with the workplace and whether or not they want to bring any union.

And there are cases that have come out of NLRB, the National Labor Relations Board, saying that some forms of blogging, some forms of internal e-mailing amongst employees, can be protected concerted activity. So before you fire somebody for blogging or sending around or complaining e-mail internally, be careful about that issue.

Another employer exposure out of the connected lifestyle is what the police are calling DWT, Driving While Talking, Driving While Texting. There have been some pretty high profiles incidents, where people have been driving down the road late at night and talking on the phone and hitting some – hitting and killing a pedestrian or there was a young lady in Northern Virginia going home from a high school graduation party texting with her friends on the way home. And hit a tree, went off the road and died.

So, the police really are behind a lot of statues and a lot of jurisdictions. California now has that. Columbia and others are at still (behind) the bandwagon. Prohibiting Driving While Talking if you don't have hands free device. And I think those statues are only going to increase.

Virginia has a law saying that, teenager can't talk or text while driving. You can't have any device, you have to be paying full attention. So, employers would be well advised to have policies, saying you must comply with the law.

You must not do these things and even if you are in a jurisdiction where you don't have such a statue, there still can be what's called a respondeat superior lawsuit. That is in the case – there was a case involving a lawyer driving down the road at night and allegedly talking to a client and hitting pedestrian while talking to a client.

So, a lawsuit was brought against, not only the lawyer, but against the law firm employing that lawyer on the theory that she was doing work with the telephone while driving. So, there can even in the absence statue, there can be a potential liability for the employer under this respondeat superior theory.

Alison Gardyne: Dan, I think – this is Allison. On that particular point too, I think that companies who issue, Blackberries or PDS or other devices, not only should have a policy but also should ensure that there are hands free devices going along with that. Because I think we've not seen claims of that yet, but if you are issuing technology to an employee to use as part of their work and do not provide the hands free device. I think that that could raise, some concerns and some potential exposure having them need to get out on their own to get that.

So, that's something to think about too. Not only have the policy that says, you should be using this, but also make sure that that's provided to the individual if you're providing that device itself.

Daniel Westman: That's really good point. Then really disturbing case and hopefully none of you will ever experience this track pattern but in the (Dov) versus XYZ Corporation case, a step father was kind of a known pornography viewer at work. You don't ask me how they didn't do anything about it, but I guess they said that's just Joe. And got a yuck out of it.

Well, the problem is it went on and on and on. He develops a proclivity for child pornography and took a photo of his step daughter unclothe, which he use to apparently the price of access to some of this child pornography Web sites was posting a photo. And he did that to gain access, using the company's computer and in the workplace.

The step daughter and x-wife, mother of the step daughter sued the company, saying the company was negligent in allowing his behavior to get so far of hand and the Supreme Court of New Jersey agreed, saying there was policy that for bad pornography over the company's computer.

The company could have taken many steps to disappoint the fellow, did not and therefore allowed him to be liable. And pegs a question about how much of an employee's internet activities does the company need to know about. That question is unanswered, but clearly if in an extreme case like this, the company was aware that this fellow had a proclivity towards these activities, which would have been stopping them and they didn't and that led to potential liability in this case.

Karla Elliott: Dan, two other, this is Karla again. Two other quick points to add for potential employer exposure in these areas that we're talking about. We want to remember too that companies might face liability for wrong copying of software and other content by their employees, back when we're looking at the Symantec survey results, how the millennials are much more likely to use the work devices for their own personal use.

I think we see that in reverse where they might well copy or download technology or software to a home device that could be used for work because of he is doing so, potentially leading to licensing or copyright infringements on behalf of the company. So that's another area to keep in mind.

And the one thing that I don't think we have mentioned that comes into play when we are talking about the devices, the texting and talking and Blackberries and cell phones. There is a lot of current litigation out there surrounding whether that time spent outside of work and outside of regular working hours doing things like checking your Blackberry or e-mail could be considered compensable time under the FLSA.

It's very much an open question in different areas in something that when we're developing those policies, you may need to keep in mind for how we're treating exempt and non-exempt employees in those circumstances.

Daniel Westman: Those are great points and some companies were aware of our only issuing Blackberries to the salaried employees to try to avoid that. But then, of course, the non-exempt people feel disrespected because they don't get the cool technology.

Karla Elliott: I mean the other approach to that is to when you do issue it, you are making it clear that you're non-exempt, that if they are checking their Blackberries or devices after working – that's work time that needs to be recorded. Clearly, whether you are going to get all that monitoring and really how you monitor that, but that is certainly something of an issue.

And it also comes up with exempt employees on the – under the FLSA, any work performed in a day counts as a day. So how many exempt employees probably any of us on the phone have ever gone on vacation and not checked our Blackberry one day, does that mean we can't be paid for the vacation, we need to be paid for the full day.

Haven't seen any cases on that, but it does raise the point that FLSA laws were written at a time when this type of technology didn't exist and either did voice mail and so the concept of somebody being really out of range and not just checking e-mail to figure out what's going on while on vacation can be raised as a concern.

Daniel Westman: OK. We are getting short on time so let me speak through the last point, which is how the generational differences maybe playing out in the workplace. The last data from the EEOC show that all categories of discrimination are up including age discrimination and retaliation some subset of which is retaliation for filing age claims.

So we don't know why that is but it is happening. A title of this case, potential glimpse into the future because Google like Yahoo, Alison is one of those companies, where the average age is probably pretty low compared to other companies. Mr. Reid was hired at the age of 52 and let go few years later and supposedly he was told that he was too slow, fuzzy sluggish. His ideas were obsolete and too old to matter.

Now as I understand the lower court granted summary judgment in the favor of Google finding that the Google employees honestly believed that he did not have the skills that they needed. We ((inaudible)) saying those are stereotypical age comments and maybe sufficient to sustain an age claim and that case has been accepted by the California Supreme Court.

So is no longer on the books but is going to be argued in the coming year. So this may become a more frequent pattern that we see where people of younger generations are supervising people of older generations and need to be trained. You can't really say your ideas are too old to matter or obsolete without begging age discrimination issues. It’s certainly not great practice even if doesn't get suit your age discrimination. Alison and Karla, any comments on that?

Karla Elliott: No. I think that we are likely to see more of those claims in the future

Alison Gardyne: I would agree.

Daniel Westman: So, the last point is that family responsibility discrimination is not a category called out in any Federal statute but it is an element of the Family and Medical Leave Act. It's an element of the Americans with Disabilities Act and other state and local statues.

And the Hastings Law School is San Francisco issued a report two years ago noting what they believe is a 400 percent increase over the decade of '96 to '05 and what they characterize as family responsibility discrimination. We are seeing a groundswell of state and local laws protecting parenthood and family status and family responsibilities, although Federal law isn't there yet.

And what that may indicate is generational tension about flexible work styles. The younger generations thinking that the older generation doesn't give them time to deal with such issues and older generations believing that the younger generation just don't want to show up during regular working hours and want too much time off. So this may be a reflection of that tension.

Another comment is that as we all age, elder care responsibility is going to fall on people of all generations and could also raise family responsibility issues. So, just as there is tension around the cultural difference around technology, there could be tension around the flexible work style or the flexible work life balance that the younger generation seems to prize more so than the older generation.

I'll just comment briefly, a couple of Stanford Law students made the headlines a year or so ago effectively making that point saying to the big law firms, we think you got to change. We think you work too hard and frankly we don't want to work for you unless you change to a style that enables more work life flexibility.

So, before I turn it over to Bill, Alison and Karla, any thoughts on that?

Alison Gardyne: No thoughts. I think you summed it up great Dan.

Karla Elliott: Exactly.

Daniel Westman: OK. Bill, would you kindly take it over and see if we have any questions from our audience?

William Harn: Sure. Thanks, Dan. What I have is one question came from an individual with regard to Driving While Texting, and if a company has a policy that prohibits such behavior. The caller or the Participant asked, can the employer escape liability, if the employee violates the policy and then turnaround and blame the employee?

Now, I don't know if you could escape liability simply, because of a violation of policy is activity occurred during the course of scope of employment, but holding the employee accountable for the employers loses as a result of their conduct is another story, any comments or a feedback on that idea from either of you?

Daniel Westman: Yeah, sure. The policy may not be enough to insulate you from liability for regular damages, but it certainly would go a long way towards knocking down any punitive damages claim, which is available to a case. So it gives the defense lawyer a great argument that this company did everything that it could to prohibit its employees from doing this and they did it anyway, so you shouldn't punish us.

In that case, I mentioned involving the lawyer got another road. The lawyer was hit for significant punitive damages in that case. It was a largest verdict in that particular county, in Virginia. So it's not – it's worth thinking about the worst case punitive damages and this policy can help you to file it off.

William Harn: I had one other quick question of my own. And that was, if any of the panelist thought there was or had some insight on managing Millennial and Gen X productivity giving their willingness to use employer technology at a whim, the 70s or 80s I remember used to get hammered for spending too much time on the phone with your buddies or whoever else and now its instant messaging and e-mail and anything in between.

Is there any suggestions you have regarding the loss of monitoring the productivity in light of technology changes?

Alison Gardyne: Bill, this is Allison, I think that that's a really hard question depending on how the company operates because as Karla mentioned earlier, IMing with customers and e-mailing with customer and going on and off Web site is part of people's jobs now and days.

And so, unless you've got a whole team of monitoring good use of that use, its difficult and I think Dan had mentioned that certainly some company will restrict the use of certain Web sites and will set up firewalls, so that you can't have – there are some companies that will prohibit access to pornography site or prohibit access to gambling sites or those types of things.

And I think you can pick your evils and ones that clearly are not part of the company, but how many admins use MapQuest or Yahoo! Maps to figure out where they are focusing to go. I mean its part of the culture now is for the using the Internet. And it's really hard to just say, as if most companies were trying to halt but you couldn't. Airlines tickets are made online. You know everything is part of it.

And so, it's really figuring out that reasonable and incidental personal use and then addressing the – when it comes an abusing situation. There are some software pieces out there, I think that will monitor just generally how much time you spent on the Internet and that might be something that you then sort of look at the real high end users and figure out, OK, what's going on here. But again, that's all part of the company culture as to how big (brother) you want to about it.

Daniel Westman: Yes, let me just, if I could, I know we're running out of time, make one follow-on comment. When we are asked to diagnose how the trade secret misappropriation or data security breach happened, often we tell clients your computer networks were configured. In fact, maybe even you enabled the parts of the network that did generate reports on anomalous usage as you say, also people whose usage is just out of the norm and either company didn't turn on that feature and get reports or they ignore the reports.

So going back to what we started off with example of the lady at O'Hare with the one-way ticket to Beijing, who copied in 48 hours, $600 million worth of trade secrets. I don't know how the company found out about, but if they had enabled their network to detect and report anomalous usage, that is one way to prevent that kind of breach or misappropriation.

And what concerns me in trade secret litigation is the judges always expect you to prove that your company took the reasonable measures to protect its trade secrets. And if my advisory says look you had computer network that could have given you this report and you didn't enable that or you didn't even look at the reports then that the judge may rule against our clients. So it's a very, very significant issue.

William Harn: Well, I want to thank our panelist for doing a wonderful job today in giving us an excellent overview and some good hands on insight into many of these issues. Dan Westman, Karla Elliot and Alison Gardyne, thank you again for your extra ordinary input and efforts today.

I would like to remind all of our participants that we have a seminar evaluation. If you would click on that link in the links box and complete that information and send it in, we would really, really appreciate it. In the mean time, I think we'll close our presentation and wish everybody a wonderful Veterans Day in honor of those who have served our country over the last several 100 years. And have a terrific week.

Everybody may now sign off from the call. Thank you.

END