Webcast: Implications and Pitfalls of U.S. Privacy Laws and Regulations
Date and Time: Tuesday, November 14, 2006 at 11:30 AM ET
Presented by ACC's Corporate and Securities Committee and the law firm of Pillsbury Winthrop Shaw Pittman LLP

Panelists: John Nicholson, Senior Associate, Pillsbury Winthrop Shaw Pittman; Colleen Vossler, Senior Associate, Pillsbury Winthrop Shaw Pittman

ASSOCIATION OF CORPORATE COUNSEL

Moderator: Jessica Wenzell
November 14, 2006
10:30 a.m. CT

Operator: Just a reminder, today's conference is being recorded. Please go ahead, (Jessica).

(Jessica): Hello, everyone and welcome to today's Webcast sponsored by the ACC's Corporate and Securities Committee. I'm (Jessica Wenzell), your moderator.

We're here to talk about U.S. privacy laws and regulations, the number and breadth of which seems to be increasing on a regular basis these days. It's an area of law that all companies need to know about whether you're public or private, big or small, B-to-B or consumer oriented.

Our two presenters are Senior Associates from Pillsbury Winthrop Shaw Pittman. Colleen Vossler practices on transactional matters primarily within the technology, financial services and non-profit sectors. She ahs structured Web sites to conform with local law and industry

best practices regarding the collection of personal information. And she's also conducted Web sites to uncover privacy law compliance efficiencies for her clients.

John Nicholson's practice focuses on negotiating complex technology transactions. And he also specializes in data privacy and computer security. With past IT experience, he can (contemporaneously) solidify practical solutions to compliance issues.

And with that introduction, I'll let the presenters get to it. We're here for an hour. You may send any question to the presenters at any time using the box on the bottom left-hand side of your screen. It's entitled "Questions." Type in your question and press "Send." Only the presenters will see the question. And we'll have a Q&A at the end of the presentation.

Also I want to note we want you to please make sure to complete the Webcast evaluation form also in the links box on the left-hand side of your screen in the drop-down menu. Please make sure you select today's Webcast entitled "Implications and Pitfalls of U.S. Privacy Law and Regulations."

And with that, it's all yours Colleen.

Colleen Vossler: Thanks, (Jessica).

Good morning, everyone. I wanted to go through a quick outline. We have a significant number of slides, if you've taken a look at the number of them. We intend to try to cover as much as we can. But many of the slides are for your reference after the presentation, so you

will note a few times that we will skip ahead when there are things like, "Multiple Enforcement Actions by the FTC.

With that I'll go quickly into the outline. What we'd like to cover today is the U.S. Federal landscape. And you'll see that we have five different areas that we'll touch on. We'd like to also talk about the U.S. State landscape, which is becoming more important on a daily basis. And then we'll lightly touch on things that are going on, on the outside of the U.S. in terms of outside our borders, and how your company may have a problem if you're not thinking fully through the type of data collection that you're doing.

Now the first thing that we're going to touch on extremely lightly is the Gramm-Leach-Bliley Act. There was a recent presentation given through the ACC. So if you're looking for anything in depth on this subject, please go ahead and refer to that. But what we just want to remind people about is that FERPA exists. It does require anyone who is a financial institution to protect two things, it's both security and confidentiality of any non-public financial information of a particular entities customers.

There are multiple agencies that are required to help coordinate the development of regulations. So it's not one agency doing all of this. It's multiple, so you might see things from different areas. And we've given you the reference, again, if you're interested in looking further.

Part of the reason we're not going into this is again it spins on, but we also wanted to spend time on other areas that may be of more interest to a wider audience through the ACC.

John Nicholson: Before we leave that, though, the reason why financial institutions is in quotes in there is because Gramm-Leach-Bliley does have a very broad definition of what constitutes a financial institution. If your organization does things that are bank-like in terms of giving loans, extending credit, things like that, you may be considered a financial institution for the purpose of Gramm-Leach-Bliley. So that's something that may be relevant to you.

Colleen Vossler: That's a good point, John, thanks.

OK. Now we'll move on to the Children's Online Privacy Protection Act, which is called COPPA. And I'd like to stress one important thing about this. This is one of the first practice tips that I'd like to impart. If you are familiar with the law, you'll know this already.

But for those who are just delving into it, one of the critical pieces to remember is you will get caught up in this law and be required to comply. And we'll talk about that in a minute. The marker is for children under the age of 13. So from 12 years, 364 days and younger, you are required, if you fall into that bracket, that's the age group that we're targeting here.

Congress basically, if you look at the law, made a distinction and said children under 13 could not adequately protect themselves online. Children 13 and older could. So it was the line that Congress decided to draw. And as a result we want to discuss that a little bit further.

First of all you might say, "Look, we don't deal with children's issues. So I'm sure that this does not actually apply to us." In fact, if you operate a commercial Web site or an online

service that is either directed to children under 13, which is the obvious ones, and you collect personal information from children, then you'll be required to comply with COPPA.

The less obvious aspect would be if you operate a general-audience Web site and you have actual knowledge that you're collecting information from children under 13, you also will be caught up under the law. Now actual knowledge doesn't necessarily mean that you are watching a child register, and you see as an individual, and perhaps as a council, that the individual is under 13. We'll talk about this in just a minute. But this can be a trick or a pitfall that you can fall into.

Now to determine whether you're an operator, FTC will look at multiple factors. You do not need to meet all of them, or have a significant number of aspects of each in order to be an operator. But they will look at things such as, "Do you control the information once it's collected? Do you own it? Are you paying for that information collection and for the maintenance of it? Do you have pre-existing contractual relationships that are in existence with respect to the information? And what role does your Web site play with the collection or maintenance of the information?"

Now let's move on and talk about what makes a site targeted to children. This again is a factors test that FTC would employ. There are multiple aspects of it. And they're going to look at things like subject matter, if there's audio/video content. When you're using a model on your Web site, does the individual look – whether or not she is fact young – does he or she look young so that you would say that it could be a peer of a child under the age of 13. Is the level of language on your site something that is very plain and directed at something you might give, say to a 10-year-old as opposed to an adult? Do you have things on your

Web site where you have advertising pieces, and it's for things that are child oriented? For example, if it is a children's television show that is being advertised, that would be one of the things the FTC would look at. We also want to look at the target or actual audience age and whether there's child-oriented features.

Now I'm going to move on, because we could spend time determining whether or not a particular organization would meet the test. But I think we need to move through so that we can give you a little bit more of a top-level picture of this law itself.

Now what is actual knowledge? This is another place where I like to give practice tips to those who are listening. If you have a registration form on your Web site, and in some way the user enters an age that's under the age of 13, then you are required to comply with COPPA with respect to the information that that user has provided.

Now this can happen in a couple of ways. First it could be that you put in your age as a user. It could be 4/24/1994. That individual would then be under the age of 13. It could also be that your Web site, when you have a registration process, has something that discusses age groups. So is it the ages of 30 to 50, 21 to 29? And then if you have something that says "under 18, under 13" so that when someone clicks on that box you know that they would be under the age of 13, or could be.

Another way to do it would be if someone is actually putting in their number of years that they have attained. So if I put in that I am 35, that would be something that you would be able to tell the age of the individual.

So be careful as to looking at your own Web site and see if you can get caught up in this unwittingly. A lot of time organizations, when I've counseled them, have decided that they really don't need the year of birth, and are not that interested in having to comply with COPPA. And rather than get that demographic, have decided to take that piece off of their registration. And therefore, because they don't meet other factors, don't need to comply.

One other thing that's another practice tip, it's not enough if you have a box that says, "under 13" or something that would be 4/24 – so April 24th, 1994 was my first example. If you just return a response to someone who's trying to register and say, "I'm sorry. You're too young to register for this site." The FTC has determined in its own working with the law that they actually need to have Web site owners be a bit more proactive. So if you have someone, if you just choose to use age and you need that as your demographic, that's fine. If someone registers and is under the age of 13, you need to do two things. Return as response that says, "I'm sorry, we're unable to process your request to register at this time. Thank you for your interest." Because you're not indicating to them what exactly the problem is. And then what you also need to do is completely purge all of the information off of your Web site so you're not retaining anything of the child's. Now I know I spent a bit of time there, but that's one of the places that I often find my clients falling into the trap of needing to comply with COPPA when they otherwise might not have had to.

Personal information is a very broad range of things. You'll see the list here. It's things that are obvious like name an email address. It's also things that are less obvious such as, if you collect information passively through cookies or tracking technology, and you're linking that information to other information that's individually identifiable, that would fall under the offices of personal information.

Now in terms of complying with COPPA, if you actual need to comply – what you need to do is, if you're a site that is directed to children, you want to have a link to your privacy policy on your home page and in each area where the site would collect personal information from children. And again, children meaning those under 13.

If you're a general-audience site, and you have a separate area that's directed to children, what you want to do is have link to your privacy policy on the homepage of the children's area. And here's another practice tip. It's not required, or it's not apparent that it's required, that you have links in other places. John and I feel that it's a good idea to provide a link to your privacy policy wherever you collect information from children, if it's personal information. That way, it's a best practice and you are on the safe rather than sorry side.

Now there are multiple exceptions to COPPA requirements. And I'm going to touch lightly on a couple of them. The others, you'll need to just sort of look at when you have a few moments. One of the first one that I think is not as obvious, if a parent is agreeing to the collection and use of their own child's personal information, the operator is permitted to provide the information to others if it's for support of internal operations of the Web site. So you don't need to be worried about not complying with COPPA if for some reason you have a technical support aspect, or order fulfillment, something like that. So I think the law, in that sense, was written intelligently because it does give these exceptions so that you can do the business that you need to do.

For sanitized information, if there is a monitored chat room and any bit of personally identifiable information is actually stripped from the posting and they're not made public,

and they're otherwise deleted, then what we would – our review of the law is that an operator is not required to get prior parental consent. And that's what the FTC has said based on the regulations and the law itself.

Now, you are not required to get parental consent in other instances. You might think that this is a bit of a circle jerk where you need to get a parent's consent to collect information about a child, but how do you get to the parent if you can't collect the information. So you'll see that one of the exceptions is that, if you're trying to seek parental consent, you can in fact use the child's email address or other personally identifiable information for the one time to seek that parental consent.

The other thing that you're allowed to do, that I think makes it easier for businesses, is to use email addresses to respond one time to a single request from a child. Or if you have a subscription aspect, you can respond more than once as long as you have notified the parents that you're regularly communicating with their child, and you give them an opportunity to stop the communication before multiple communications occur.

Now once again, this requires some thought on your part in terms of how you're actually developing your system. What you need to do is have a system that notifies a parent before second communications are sent. And that the system also has the capability to cancel a second communication if in fact the parent does not give consent.

I think we will continue here with exceptions, because I think we have the time to do that. For prior parental consent, you don't need to get it if the Web site is going to protect the safety of a child who's participating in the site, or if it's with respect to the security or

liability of the site to respond to law enforcement. So these are the sorts of exceptions that you see in other laws as well. And again, it makes sense for the Web site to be able to use them in these narrow instances.

If you go ahead and change your collection practices with respect to information, it's very important to note that you cannot rely on the old consent given by a parent when there's a new practice, if it materially changes the collection user disclosure of the information.

So once again, if you are collecting information about children, you need to develop a system that works in the following way. There are other ways to do it, but John and I feel that this is one of the better ways. Track the child by the date that the parent has provided consent, the uses that the parent has agreed to with respect to the information, and then also a method of contacting the parent if the use that you've specified actually changes.

All of these are somewhat cumbersome. They can be expensive depending on your implementation. If you were looking to collect information from children, and you have a business need to do so, these are what needs to be factored in to your decision to collect that information in terms of time, money, effort et cetera, so that you can stay on the correct side of COPPA.

Now if a parent contact you, you need to do two things. One, if they make a general request, you're required to tell them the types of information that you generally collect. If they make a specific request about the information you're holding on their child, what you need to do once you've verified that it is in fact the parents that is asking about their own child, you need to give the specific type of information that you have collected over time.

Parents, it's very important to note, can revoke consent at any point, and request deletion of their child's information. So that's something to keep in mind as you look at actually engaging in some sort of system for the collection of information.

You want to obviously do everything aboveboard, not just because it's the law, but it's also the reputation of your entity, which you all know. If a parent gets uncomfortable for any reason, whether it's how they think the information is being used, they just feel that their child may be giving too much information, they can contact you. And your obligation is to comply with their request with respect to not using it, deleting it, terminating the child's privileges.

The one caveat to that is, if you offer a particular aspect of your Web site that is not contingent on the information, the personal information that the parent has asked you to delete, what you want to do is allow the child access to those portions that don't require personal information, and prevent them from accessing the portions that would require something, say like an email address. So there are still ways to allow the child to legitimately go ahead and participate.

Now everyone who's sitting here hopefully realizes the importance of complying with COPPA. I think one of the startling aspects of it has been the level at which the FTC has sought enforcement actions. It is mind boggling in terms of the money that organizations have been assessed as fines and penalties.

Each time you violate COPPA, it is up to $10,000 per violation. What that means is, if you have 30 children about whom you've collected information, and you've not received – or excuse attained the correct parental consent, that's $300,000 that you could be potentially fined. The fines add up pretty quickly, particularly if you're targeting a specific segment of the children's population. And you might find that you have millions of users who've signed up.

One great example is the most recent no parental consent enforcement action that the FTC engaged in. And this is against a company called Xanga.com. This is a $1 million penalty that the FTC fined Xanga. It's the largest that was ever assessed to this date for violations of COPPA. And basically, Xanga.com is a social networking site. It's similar to MySpace, for those of you who are familiar with MySpace. And the FTC charged that they allowed the creation of 1.7 million accounts for users where those users submitted birthdays saying that they were under the age of 13.

The company took this fairly seriously. And what you see with my last two bullets are ways that the company has tried to improve on its actual performance on an ongoing basis. What they've done is address the violations, added additional safeguards so that they could prevent children under 13 from registering on the site. They've also hired a new chief safety officer and added personnel to respond to complaints from parents.

Now while a lot of that is probably a reaction to the FTC's investigation, this is another practice tip that I always impart to my clients. It's so much better to be in compliance rather than not in compliance and become a poster child for the FTC.

The FTC – as you'll see, we're going to skip through a few other enforcement actions in the interest of time. But what you will see is that the FTC has gone after some very large entitles. They've gone after Hershey's, Mrs. Fields. What you want to do is review your own practices, see if there's a chance that you might need to be compliant with COPPA if you were to review them either on your own or with the assistance of outside counsel to determine that you're actually not in compliance with COPPA.

John and I have sat in on talks with the FTC where the FTC has been very up front and said, "Look, yes we need to go ahead and enforce COPPA. However, we want organizations to come to us if they think that they're not compliant." So you could conceivably give the FTC a call and say, "Look, we're afraid that we're not compliant, or we know that we're not compliant. We want your help because we want to become compliant." They were not able to release us the names of the organizations that they were working with. But they indicate that those are the phone calls that they welcome. They try to help the organization work through it. And as long as you're doing it in good faith, it's much better to probably engage in that rather than wait for the FTC to find you and again make you the poster child.

So what you'll see on the next several slides are different enforcement actions that the FTC has engaged in. Again Xanga was a $1 million. So each year it seems that the amounts are going up as the companies has more growth violations of COPPA. And that's a big hit to your bottom line.

Now what we're going to do is turn it over to John right now, who's going to talk with you a bit about FERPA. And with that, John, I'm going to hand it to you.

Operator: John, make sure your phone is unmuted.

John Nicholson: There I was waxing eloquent without turning off mute.

Since we were talking about children, we figured we would touch Federal Educational Records Privacy Act, which is the law that protects privacy of student education records. Those of you who are already involved in the educational world probably already have intimate experience with FERPA. But FERPA applies to all schools that receive funds under a program from the Department of Education. And you can find the relevant regulations and a policy guide at the link that's on the page there.

The important thing about FERPA is that parents or eligible students have the right to inspect and review that student's records, and request that a school correct records and have a hearing regarding disagreements over them. So when you were a child, or what you've told your children that something will go down in your permanent record, this is the permanent record that you have an opportunity to review and correct.

Outside of that, schools have to have written permission to release educational records with some very specific exceptions that are covered on the Department of Education's Web site. Schools are allowed to release directory information, but they have to inform the parents and the students that, that directory information is being released.

So if you are receiving Department of Education funds, and providing education to students, you should not display students' scores or grades publicly in association with names, social security numbers or other personal identifiers. Assigning a student an

anonymous grading number and posting that is acceptable. Don't put papers, or graded exams, or reports with names or grades in publicly accessible places. Don't just put them on a table outside an office and let students come pick them up.

Don't share student educational information including grades with parents for others outside the university, including letters of recommendation, without the written permission from the student. And for those of you who are parents, one parental-practice tip is that you can obtain that written permission from your student. What you do is you – for college students for example – you trade the tuition check for that semester for a letter providing written permission from the student.

From there we're actually going to go on HIPAA, the Health Insurance Portability and Accountability Act. And HIPAA authorizes the Department of Health and Human Services to adopt standards that require health plans, healthcare providers and healthcare clearing houses to take administrative, technical and physical safeguards to ensure integrity and confidentiality of health information, and protect against reasonably-anticipated threats, unauthorized use or disclosure of that information, and to ensure compliance by officers and employees. And the reason – like (GLIBA), the reason why health plans, healthcare providers and health-care clearing houses are all in quotes is that HIPAA provides very specific definitions of those that may go further than you think they do.

Health-care entities have to implement new privacy policies, comply with certain specific technical security requirements, provide notice or secure authorizations for certain uses and disclosures of information. And they have to enter into written agreements with business partners that are called business-associate agreements.

The security requirements under HIPAA fall into three general categories – administrative safeguards, physical safeguards and technical safeguards. Administrative safeguards are the policies and procedures associated with protecting individually identifiable health information. Physical safeguards are locks, screens on computers, things like that. And technical safeguards are the technical means by which you protect information.

HIPAA does provide descriptions of what an organization must do, and how it must be done. But it does not specify particular technologies. Under the HIPAA documentation requirements, a CEA-covered entity must maintain documentation about your policies and procedures until the latter of six years from the date those policies or procedures or created, or six years from the date that the policy or procedure was last in effect. So if you change your policies or procedures related to keeping HIPAA information secure, you have to keep a copy of that policy for six year.

You might be surprised about who is a healthcare company. If your company self-insures, it's conceivable you could work for a healthcare plan. And you may be required to comply with HIPAA even though you wouldn't consider your company a healthcare company. You company might also be a business associate of a covered entity, and therefore subject to HIPAA through a business-associate agreement. T

The other reason why HIPAA is important to non-healthcare companies is that because a great deal of thought when into the system for identifying protecting information under HIPAA. Other regulatory frameworks may attempt to piggyback off the HIPAA model. So in the U.S. our privacy model tends to be industry focused. We have financial privacy

regulations, healthcare industry privacy regulations, educational privacy regulations. If another entity were to try to handle another tower of industrial regulation, then it's possible that they might try to use the HIPAA model. And it could become relevant.

As Colleen mentioned, the Federal Trade Commission is moving forward and being very aggressive in the privacy space. They are addressing COPPA compliance, as we discussed earlier. They're also going further and enforcing both privacy policies, and they're creating a de facto standard for acceptable security. And the way the FTC does that is they claim that failure to take reasonable security precautions to protect customer data is an unfair practice that violates Federal law.

And I'd like to walk though a few enforcement examples to show how the FTC is moving forward in this space. Most recently, Designer Shoe Warehouse, DSW, announced a data breach relating to a million-and-a-half credit and debit cards, and 100,000 checking accounts and driver's licenses. The FTC claimed that because of the way that DSW was processing data. DSW had wireless networks within their stores, and credit-card information and checking authorization information was traveling unencrypted via these wireless networks. They were able to be accessed by a couple of individuals who just went into a DSW store with appropriate equipment to pull that information out of the air. And because of that, they were able to commit fraud and identity theft using those credit-card numbers and checking-account numbers.

So the FTC claimed that DSW created unnecessary risks to sensitive information by storing that information when DSW didn't need it anymore. DSW supposedly failed to use readily available security measures to limit access to its networks. They did not encrypt the

transmissions for example. They stored data in unencrypted files. And they failed to limit the ability of computers in their in-store networks to access the Internet. They also failed to employ sufficient measures to detect unauthorized access.

Based on FTC's investigation, they settled with DSW. And among other things, DSW had to commit to implementing a security audit, from a qualified independent third party, every two years for the next 20 years. That's both an expensive prospect and a fairly painful one. But that seems to be FTC's standard practice at this point in security cases like this.

Similarly, card-processing systems – Card Systems is an entity that processes authorizations for credit and debit-card transactions. And a computer cracker used a very common attack, one that was well known in the industry, to break into Card Systems Web site and install malicious software to collect information off of Card Systems network. The cracker got access to tens of millions of credit-card numbers that were then used to make fraudulent transactions. And again, the FTC required them to implement a comprehensive security program and subjected them to an audit every two years for the next 20 years.

In both of those cases, DSW and Card Systems did not necessarily violate their privacy policies. They simply were subject to attacks that the FTC said were reasonably predictable and could have been prevented through reasonable precautions. That level of security is becoming a de facto standard. And the FTC is enforcing that on other entities.

Since we've been talking about data breaches, we'd like to move into a discussion of U.S. State laws related to data breaches. And as of now, roughly 33 states – and I say roughly because this is an area that's moving very quickly. A number of states still have data-breach

notification laws that are being considered. And you never actually know when the next one is going to be passed. Right now 33 states – there is no Federal data-breach notification law. But think back to what I just said about the FTC enforcing security promises related to data breaches.

The State laws have varying requirements and varying definitions. And that creates a problem for multi-state organizations. The trigger for action under the various State data-breach laws can be knowledge based or risk based where there is a risk that information may be materially compromised or there is a likelihood of harm. Knowledge based just means you know that information was exposed.

The State laws vary in that they may apply to corporations, state agencies or both. They may exempt HIPAA or (GLIBA) regulated entities or other entities that are subject to similar State laws. For financial institutions, they may tie to the inter-agency guidelines issued under (GLIBA). They may apply to entities only within the state. Or as we'll talk about in the case of California, may apply to any entity that has data about the citizens of that State. They may exempt entities from notice requirements if the entity has its own notification procedures. And 25 of the 22 laws that are currently in place have some level of exemption.

So as you can already see, this is a complicated field. And if you operate in multiple states, or you have members or customers who are in multiple states, you may be subject to one or more of these laws. And because there is no preempting Federal law to give guidance, you may have to deal with multiple conflicting laws.

Going on with some of the differences between the data-breach laws, personal information isn't uniformly defined. For example in Montana, only a Social Security number is considered personal information. In Arkansas, the definition includes medical information when it's combined with a name. In Georgia, it would include any password or other identifier that permits access to an account without the name as personal information.

But in Georgia for example, the law only applies to data brokers. Most state's state laws permit enforcement by the State's Attorney General, but are silent on private causes of action. However, Washington includes a private cause of action for injunctive relief and damages. Florida includes penalties for failure to give notice. Notification periods aren't uniform, nor are the exceptions for delaying notice. Some states provide opportunity for you to delay notice if it's part of a law-enforcement action. Some states require immediate notification. Others require prompt or timely notice. So again, you may be subject to different or conflicting requirements.

One thing I would like to talk about that is not in the slides that just came out late last week – there's an organization called the Ponemon Institute, that surveys privacy practices and privacy laws. And they have just completed their annual survey of the costs of a data breach. And what they determined is, on average for data breaches that took place during 2005, the total cost averaged $182 per lost customer record, which included direct costs of $54 a record, lost productivity of about $30 a record and customer opportunity costs of almost a hundred dollars a record. Where those customer opportunity costs came from are that almost 20 percent of customers who were subject to a data breach terminated their relationship with the company. An additional 40 percent were considering terminating their

relationship because of the data breach. And according to the Ponemon Institute survey, only 14 percent of them were not concerned about a data breach.

So for the purposes of your customers and members, dealing with data breaches and being at risk for data breach is a very serious issue. And once again, the name of the institute is the Ponemon Institute. That's Ponemon. And you should be able to find them online. And if you give me just a second I'll give you their URL, or we'll answer that in questions.

I wanted to talk specifically about the California Security Breach Information Act, which was the first one and was the reason why the ChoicePoint data breach became public knowledge a few years ago. It went into effect July 1, 2003. And it mandates disclosure of breaches in which confidential information of any California resident may have been compromised. And I need to reiterate that – any California resident. It does not apply to California entities. It applies to the data of any California resident. Now this hasn't been tested. But California's philosophy is that they get to protect their citizens.

So if any organization has one customer or one employee in California, or if you're an outsourcing company that's doing work for a company with customers in California, or if you store data for companies with information on California residents like ChoicePoint did, then effectively, any person or organization in the world that stores data electronically and does business in California, you may be subject to California's security breach information act.

The SBIA covers unencrypted personal information that's acquired or reasonably believed to have been acquired by an unauthorized person. And there is a description for what

California considers to be personal information. And it's pretty broad. What you have to do is notify California residents in the most expedient time possible, and without unreasonable delay. The law also provides – I see somebody else has provided the Ponemon link in the questions frame. Thank you very much.

The law does provide for notification in terms of written notification and electronic notification. Or you can follow your own notification procedures as long as they're documented as part of your information security policy. If the cost of notification is excessively high, i.e. greater than $250,000, or the number of people you have to notify is more than 500,000 or you don't have enough contact information, then you can send email. You can make a conspicuous posting on your Web site. And you have to provide notification in major statewide media.

If you fail to disclose a security breach under the SBIA, you could be liable for civil damages and class-action lawsuits, and as I discussed before, public embarrassment and potentially your business.

Got a clip here from the Associate Press. ChoicePoint stocks sell nine percent after the data breach. If you're organization is subject to a data breach, then you could be hit with similar consequences in addition to potentially fines from the FTC or other penalties, depending on which State laws you're subject to. But even if you comply with all of the notification provisions, you still might be hit by the public.

With that, I'd like to turn it back to Colleen to talk about some of the other State laws that you may be subject to.

Colleen Vossler: Thanks John. I appreciate it.

OK. Any of you remember my first outline slide, which said that we were going to talk about other State laws? In reality, California has taken the lead in many aspects of both privacy and data security. And so that's why we focused on those laws.

John did a great job of talking to us about states that include stated security laws. The reality is, with respect to privacy, California is the leader. And that's where we look when we're trying to find a common denominator for creating a privacy regime for an organization.

One of the laws that I'd like to talk about is AB 1950. It became effective almost two years ago now. And it requires a business, if you store personal information about a California resident, you need to take reasonable security procedures and put practices in place that are appropriate with respect to the nature of the information. The goal is to protect it from unauthorized access or use.

If you also disclose personal information about a California resident to a third party as part of a contract, you have to require that third party to also implement the same or similar security procedures and practices to protect the information.

Now as John asked earlier, you're probably thinking, "My organization isn't in California. Why would I care about this?" Once again, California has taken a very broad view of how they choose to protect their citizens. And it applies to – the law applies to any business that

either owns or licenses personal information about a California resident, and any company that would contract to receive personal information about a California resident. So if that could potentially impact you, you need to look carefully at this law.

The other law, another law that I'd like to talk about quickly is California Shine the Light law. There are a few exceptions to the law itself. But generally it requires a business, if it discloses personal information about a California resident to a third party, and the business knows, or reasonably should know – so again it's not the actual standard – that the third party would use that personal information for direct marketing standards. What you get is a right for the California resident to request and receive details of how that information was shared. So this gives an affirmative right to residents of California who feel a though their personal information may have been used in a direct-marketing aspect. And you'll need to comply with that as well.

You'll note that SB 27, Shine the Light, does not address legal requirements for disclosure of information. You would look to other laws with respect to that. This focuses solely on giving consumers the right to know how their information was shared and by whom.

So again, we come back to the same question, "Why do I care if my organization isn't in California?" If you are a business that has an established business relationship with a customer who is a California resident, and you meet other requirements of the law, then this law will apply to you.

Now it's important to note that, when you think of a business relationship and you think of some of our civil procedures classes eons ago, you might be looking for some sort of nexus,

things like that. A business relationship here does not mean that anything has been consummated. It simply means that something has been contemplated. So basically if you collect information about a California resident, you'll be caught up under the law.

Here's my favorite twist for the presentation today. This is not to be confused with COPPA that we discussed at the Federal level. But California, although they're very creative, failed to really come up with a great distinguishing name for their online privacy protection act. So in parenthesis you'll see that people refer to it as the California OPPA Law. So we'll just call it OPPA.

Basically, we need to look at who it affects. It affects people like the Federal (COPELA), who operate commercial Web sites or online services, if you collect any personally identifiable information on any consumer residing in California – this is regardless of age. So if you collect that information, you are again subject to the law.

So what's the practice tip on this? What do you need to do? Well what you want to do if you operate the commercial Web site or an online service, you need to do two things. First, you conspicuously post a privacy policy and you comply with the terms of that policy.

Now the second aspect of that probably seems fairly self-evident. I can't tell you how many times I've counseled clients with respect to developing a privacy policy for them. We've talked about it at great length with not only legal, but people in marketing, people on the business side, people on all aspects of the company. They put the agreed-upon privacy policy in place. And a couple of years later, someone comes back to me to discuss it. And

when we engage in any level of an audit, then all of a sudden we're finding out that they in fact didn't comply with what they stated in their privacy policy.

This would not only run you into problems with California. It will also run you into problems with the FTC. So that's something to consider as you're – even if you have only one take-away from today, is making sure that not only do you post your privacy policy, but you comply with whatever your stating. As I tell clients all the time, if you tell me that for every bit of information you want to collect, you want to sell, rent it or otherwise get money for it from any third party that will pay for it, if that's your business operation, that's OK. We need to – assuming that it's not financial, or health or children's information, we just need to put consumers on notice so that when they use your Web site they use it knowing that the information that they're giving will be used in that way.

And I think that, that takes people by surprise because I think the tendency oftentimes is to try to minimize the uses. You want to be very forthright with your uses and whatever you say that you're going to do in your policy.

Now the policy itself must contain a few aspects. You need to describe the type of information you're collecting, if you're going to share it with third parties, even if you may share it with third parties. May is usually the way that we suggest you write your policy so that it gives you flexibility. You want to describe the process for a user to review the information that you've collected about them, if you have such a process, the way that you'll go about communicating any material changes to the policy itself and the effective date of the policy.

Now this lines up somewhat with the FTC's pronouncements on their information principles. What you don't see here is the FTC also suggests that you have a security piece to your privacy policy. And that would describe the type of security that you utilize to protect and safeguard information. Based on what John suggested earlier, you don't want to make promises that you can't keep. And you don't need to be overly specific in your privacy policy. But simply discussing the level of security, or type of security in many instances would be sufficient. So that's one aspect that you would want to discuss in your privacy policy to be compliant, not only at the California level, but also at the FTC Federal level.

I do want to take a moment to remind people that we've talked about (GLIBA), COPPA, HIPAA, FERPA. So those are the Federal level privacy laws. Unlike other countries, we don't have an over-arching privacy law that would cover personal information. John's going to talk about other countries in just a moment. But what the FTC has come up with again are the fair information principles. They are suggestions for best practices as to how to structure your privacy policy and your practices surrounding the collection of information. And while the FTC doesn't have a law to hang its hat on, oftentimes it will use SEC 5 under Unfair and Deceptive Trade Practices to go after an organization, particularly if it's a somewhat egregious departure from their own privacy policies. So keep that in mind, that while there isn't a law, you still have a lot of best practices out there that are wise to follow.

Now what does conspicuously post mean? It basically means several – there's several ways to look at it. Posting it on the home page or the first significant page, using icons that are distinguishing in character, using text links, functional hyperlinks, those are ways that you can distinguish and note that you have a privacy policy.

Now there are some remedies and penalties that go along with this. The operator will have a 30-day grace period once it's notified that it is not compliant in terms of posting the privacy policy. And you can be subject to the law if you fail to comply, either in a knowingly or willfully way or negligently and materially. So again, something to think about in terms of the reach of California Law.

As John said about the data security laws, a recent check, as recent as last week, showed that none of the three laws that I've just discussed have also been tested in any substantive way. So we expect that there will be case law on those, particularly with respect to application outside of California. But those battles are coming, and we certainly don't want your organization to be at the front of that battle.

Now with that, I'm going to turn it back over to John to talk about privacy outside the U.S.

John Nicholson: Thanks, Colleen.

As Colleen mentioned, the U.S. is not the only country with privacy laws. And other countries have been very active in this area as well. The most consistent model comes from the European Union.

And I'm attempting to advance this slide. But I could say, "Next slide please." Thank you.

The European Union Data Protection Act was enacted by the European Parliament, and covers all personally identifiable information in Europe. It does not specify by industry like

(GLIBA) or HIPAA does. But it's implemented by countries on a county-by-country basis. So there are significant variations from country-by-country.

The UK is generally considered to be one of the most laissez-faire or lax in its enforcement. Whereas countries like Spain, Germany and the Netherlands are the most stringent. The philosophy behind European privacy law is very different from the U.S. philosophy. It is an opt-in philosophy where you must affirmatively give permission for your information to be used, rather than an opt-out philosophy. If your organization extends across international boundaries and particularly into Europe, and you intend to access any personally identifiable information that comes from a European, you should consult an expert in this area.

And international data privacy is a subject for another conversation. We just wanted to let you know that it was a risk that was out there and something to be considered. Most other countries outside the U.S. have followed the EU model. There are a few exceptions. Canada has taken sort of a comprise approach between the two. But again, it's like state data-breach laws, it's an area where the laws are frequently mutually exclusive. They contradict each other, and they can be a minefield for the unwary.

With that, we'd like to conclude our presentation. And there are a few questions that we received. The first of which was a question regarding determining whether a covered – or whether a company is a covered entity under HIPAA. And I'll be placing a link to the Health and Human Services Web site into the question page. And there we go. If you want to – hopefully that worked. If you want to determine whether or not your entity is a covered entity for self-insurance purposes, the link that came up – I hope is coming up soon – for CMS – if not I'll try it again. But the Web site is www.cms.hhs.gov. And from there you

can find decision tools to determine whether or not a self-insured business is a covered entity.

Colleen Vossler: John, I'd like to jump in for a minute and make sure we have time for another question that came in. One of the questions was whether or not an individual entity is covered under COPPA. And I do realize that I was moving rather quickly through COPPA. That is a presentation that we could, in terms of really covering it in any significant way, we could spend the better part of a day on that to really prepare organizations.

Something to keep in mind – and this is not only for the individual who asked the question, but for everyone. The example that was given is if you have a Web site that's fairly, clearly aimed at adults – for example, career oriented – what duty is there to find out if children are accessing it?

It's one thing for a child to access a Web site. With respect to a child's sharing information, if you are not targeted at children, and you don't have any aspect of your particular Web site that would indicate to you that a child would be using it, such as the birth date box – and remember I gave you three different ways that you can determine whether or not someone is, in fact, under the age of 13. So if you're not collecting that information, and some 12-year-old signs up for a career-oriented Web site, but you have no way of knowing that, the FTC is hard pressed to come after you. They may still knock on your door. You may have to answer some questions. But in that instance, for a general-audience site without a children's portion, and where there's no actual or should-have-known-type knowledge with respect to a birth date, you're basically OK and will not need to comply with COPPA.

John Nicholson: With that, I'd like to address one last question, since we're almost out of time. "What are the prospects in 2007 for Federal breach law, given the recent changes in the House and Senate?" This is something that several Senators and newly elected Representatives have expressed as a desire. However, this has been a desire at the Federal level for several years. There is probably more of a chance that something might happen this year. But with Federal law, the problem is always the sausage that comes out the other end of the tube. And the best example of that is the Canned Spam Act, which is not a raging success. So even if we do get a Federal breach law, it may not be what people necessarily want or would like. But there are probably better chances for it this year then any time in the past.

(Jessica Wenzell): So with that happy note, unfortunately we're out of time. For those of you who asked questions and we didn't get to them – and there are a couple of them – what we'll do is, we will answer the questions off line. And the archive of the Webcast that goes on to the ACC Web site will include the answers to those questions.

So thank you all for attending today's Web cast. We hope it was informative and not terribly overwhelming, as often the review of privacy laws is. Just a reminder that w would appreciate your completion of the Webcast evaluation found in the links box on the left-hand side of the screen.

I want to thank the ACC Corporate and Securities Committee for sponsoring the Webcast, and Pillsbury Winthrop Shaw Pittman for then participation.

If you'd like more information on the ACC Corporate and Securities Committee, you can contact (Jacqueline Winley), whose information is on the slide you're looking at now. And going to the Pillsbury Web site is in the links box on the left-hand side.

So thank you so much.

END