MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Privacy Roundtable

January 2007

Related Practices:

- Privacy and Data Security

PDF Version

Lost laptops and data-security breaches have made headlines over the past few years, making privacy a critical issue for many companies. In this month's roundtable our expert panel of in-house and outside counsel discuss the challenges of setting up privacy programs, handling the media when a security breach has occurred, monitoring employees' email and Internet usage, and creating a privacy program to deal with different privacy standards throughout the world. The attorneys are Sharon Anolik of Blue Shield of California, Philip Gordon of Littler Mendelson, Peter Lefkowitz of Oracle, and Miriam Wugmeister of Morrison & Foerster. The roundtable was moderated by Chuleenan Svetvilas and reported for Barkley Court Reporters by Krishanna M. Derita.

Moderator: How do you advise your clients to set up programs that effectively respond to unauthorized access or acquisition of a company's personal information?

Anolik: The most effective privacy programs are those that are set up proactively, rather than reactively. It is important to develop a comprehensive privacy incident response program now; the time to figure out how to respond to an incident is not after you had your first one. I try to involve many different business units in the privacy incident response planning process and then make sure that each person on the team understands their role. You need the right team in place to make sure that you can quickly and effectively respond to a breach.

Moderator: And within Blue Shield of California, which internal departments are involved?
Anolik: Our Privacy Incident Response Team (PIRT) consists of representatives from the privacy and legal departments, human resources, facilities, both external and internal communications departments, the IT Security department and, of course, the relevant business unit that may have been involved in the incident. Those departments are the constant core members of our PIRT, and then we involve additional members or departments as needed.

Lefkowitz: You have to build your team. I would add senior management of the company to the list of key players. In any of these situations, there will be tricky issues that require management judgment. It's also important for the lawyers to get involved early. We are trained to ask questions, and, particularly where the lawyers generally are not pure technical staff, we can ask people to give us details in lay language and boil things down so that we understand them and can help explain them once an incident has been resolved.

Wugmeister: I also tell clients to take the time now to look at their third-party contracts. For any service provider that is allowed to touch the company's data or customers' data, make sure that there is really good contractual language that says if there's any unauthorized access or acquisition of that data, the service provider must tell the company as soon as possible.

I also remind clients that four states deal not only with computerized data, but also with information on paper. Hawaii, Indiana, North Carolina, Wisconsin, and the GLBA (Gramm Leach Bliley Act) standards all apply breach notification rules to information stored on paper as well as in computers. We all are so focused on thinking about lost laptops and hackers, but several statutes deal with

information on paper: for example, personnel files, or the customer records that you have printed out. One of my favorite breaches was a newspaper company that printed out credit card transactions and those printouts were then used to wrap newspapers and delivered.

Gordon: It's important to identify who the team members will be and what their respective roles and responsibilities will be. Very often, the situations are fluid, and roles and responsibilities can differ depending upon the nature of the breach. For example, if it is a hack incident, the IT department is going to play a far more important role than if it's a breach involving paper documents.

It's also a good idea to work through at least one or two hypothetical situations in advance of the breach. The most obvious one is a stolen or lost laptop. Just sit down as a group and discuss, 'Okay, what will we do? Who is responsible for talking to the media? To law enforcement? Who is going to lead the IT team? And who is going to translate their results into information that the PR group can use?'

Incident response planning should include training or employee awareness to give employees some tools to help recognize a breach or potential breach that's not as obvious as a stolen laptop. For example, unusual computer operations might indicate a hack which should be reported to the IT department. Working through authorization in advance is also important. I've been involved in several breaches where the incident response team decided what needed to be done but no one on the team had sufficient authority to approve it.

Moderator: What do you advise clients about handling the media when they are dealing with a security breach?

Wugmeister: The way in which the media is handled is very different depending on whether a client is a consumer-to-consumer company or a business-to-business company. For example, in four states right now - it will be six - you have an obligation not only to notify the individuals, but also state regulators. So for example, in New York, you have to notify the attorney general and in New Jersey, the state police, when there is a breach.

Many clients feel that it's better that those notices come to state regulators before the individuals are notified not only because it's required by law in some states, such as New Jersey, but also because they think it's a lot better to have Eliot Spitzer hear about it from the company rather than a newspaper, We work very closely with our clients' internal and external corporate communications people to make sure that the notices go out to the individuals, to the newspapers, and to the regulators in a coordinated manner.

We frequently draft telephone scripts or Q&As for the call center people who are going to get calls from the individuals, the newspapers, or the regulators, Then everybody understands what happened, what the ramifications are, and what benefits are being offered so that individuals can be provided as much information as possible.

Anolik: Another helpful practice for savvy media handling involves working internally to develop-prior to an incident-approved call scripts, talking points, FAQs, and even notification letters that can be used as a basis for the documents that will be needed quickly in the event of an incident. Having these communication documents drafted and approved ahead of time facilitates smooth and fast response time.

Lefkowitz: It's also quite important to know when in the course of events to start disclosing-and not to disclose-information before the leak is under control. You have to make certain that the leak is not continuing, that it can't be exploited, and that you've put in place either a temporary or hopefully a permanent fix for the issue.

A variety of people-investor relations, customer relations, various lines of business, legal, and security-need to understand not only what the problem was, but also how you implemented the fix. Customers will want to know that you did the broadest investigation possible, but also that you have changed things from their original condition sufficiently so that it can't happen again. With my various groups internally, I try to make sure its clear not just that there was an issue and we fixed it, but how we went about that process of assuring that we had done a full investigation, and how we now have some certainty that that event will not happen again.

Another issue is looking beyond legally required disclosures. You have to think about employee and

customer trust. Sometimes it may be appropriate to cast the net a little bit wider. You may have the choice between somebody finding out from you after an event happens that you fixed it and that you believe it can't happen again, or finding out from a state regulator, the media, or a review of IT system logs. Generally, I'd prefer that they find out from you. Then you have a chance to explain it. Under that circumstance, people tend to be understanding.

Gordon: You never want your company to look like it's engaging in some type of cover-up. At the same time, the decision to notify is not so much about the timing, but whether notice needs to be provided by law because there is a difference among state notice statutes in terms of when the notice obligation is triggered.

Some states include a materiality standard in describing whether notice is required. In other words, notice is required only if the breach poses a material risk of identity theft or a material risk that an unauthorized person has acquired personal information. If you send out a notice when there isn't a risk to the consumer or to the employee: one, you might be making it less likely that the recipients will react appropriately when there is a significant risk to their data, and two, in the notice, one almost always writes that the recipient should take steps to protect himself or herself-such as monitor credit response or cancel affected accounts-and those are time-consuming and disruptive steps. The bottom line is to exercise caution before sending out the notice so you are not yelling 'fire' when there really isn't one.

Wugmeister: If you have a breach that affects people who do not reside in the U.S., the issues are substantially more complex. For example, the Japanese data protection law has a breach notification provision. It's the only other country that currently has one, and there is no materiality standard in that law. So the analysis relating to a breach for people living in Japan is really quite different, and if you have people in Europe who may be affected by the breach, obviously, the letter that you send out has to be different because the information that Philip [Gordon] was referring to would have no meaning to most of the people in Europe. You also have to be careful because the mere fact that there is a breach may cause liability to attach in some other countries.

Anolik: Certainly, determining legal requirements are an important step in responding to a privacy or security breach, but it is only one aspect to consider. Privacy is more than a compliance issue. It's about brand and reputation, and trust and values. And while companies need to, of course, look at the relevant legal requirements impacting them, they also need to ask themselves: What are our company values and where does privacy fit in? How do trust and brand and reputation impact our customers' relationship with us? The answer to those questions can be very influential when making a determination of whether or not to provide notification in the event of a breach.

Moderator: What are some of the considerations that go into setting up programs around the world to monitor employees' email and Internet usage?

Wugmeister: In the U.S., we generally say that employers have to remove the expectation of privacy, that if you successfully do that, then you are relatively free to monitor. That's true, for example, in Japan as well, but that's not true in Korea. If you don't properly deal with the privacy issues with respect to monitoring employees in the workplace, even if it's the company's computer and it's on company time, it can be criminal.

In Spain and France, if you monitor and you don't have the employee's informed consent to do that monitoring at the time the monitoring is occurring, you may not be able to use any of the information that you've obtained. They have a 'fruit of the poisonous tree' rule that applies if you don't obtain valid consent. The big mistake that U.S. global companies make is taking their policy that says, 'We can monitor any time we want' and making it a global policy. That doesn't work. I work with clients on trying to figure out how to balance the need to monitor with the need to comply with the laws of many different countries.

Companies can draft a technology-use policy so that it takes into account the different national laws, not just U.S. law, and then roll it out globally. Many clients are putting up a pop-up notice when employees log on to the computer system so that they can be confident that people are periodically being informed that monitoring will occur.

Lefkowitz: With respect to email and Internet monitoring, in the context of an approved investigation, it may be appropriate to do limited monitoring. But the investigation example really points up the need to think about what you are trying to accomplish, what your goal is, and then how you go about doing it in a way that is proportional both legally and ethically for your company. For example, are

you going to use software to monitor email? What does that software look for? If you are looking for pornography and you search email for skin tones, are you going to be pulling down people's family vacation pictures? If you are looking for 'a propensity for violence; how broadly do you have to cast the net on email content?

There are also questions to consider around how you treat the information you gather. Who's going to look at all of this? How is it going to be stored? And then there is a series of tricky employment and trust issues. When you find things out, do you have to go after every offense? If you find out things that have nothing to do with work but are illegal or improper, do you have to take action? Do you have to inform the police? Are you, in essence, becoming the police yourself? And if you are doing all of this and have made sure you have notices and consents, can you develop a trust relationship with your employee base when you are monitoring and actively reviewing every email in the interest of having a compliant work force?

Anolik: You also need to make sure that the person who will do the monitoring is trained to review information in an appropriate way. If you are giving an employee access to other employees' records for purposes of reviewing their email content or Web surfing history, you want to make sure that that person is trained in not just what they are looking for, but also in what is appropriate to do with that information.

Gordon: One important aspect of monitoring is for the HR department to remember that just putting your policy in place is not enough. There must be coordination between the IT department and the HR department. IT needs to provide HR with the information it needs to make decisions about how to respond to potential employee abuse. There was a recent case decided by the intermediate appellate court in New Jersey where an employee of a company was accessing child porn sites and actually posted pictures of his stepdaughter nude and seminude on a child porn site from the work place.

There was some indication from the IT department that this employee was engaging in inappropriate conduct, and the employee's supervisor took a look at his browser, but there was not enough communication among the decision makers on how this situation should be handled. The employee had his wrist slapped, but neither his privileges nor his job were terminated. Ultimately, the mother of the young girl sued the company alleging that it was negligent for falling to stop the stepfather's, her ex-husband's, child porn activity.

This case opens up a potential Pandora's box for a lot of companies. What happens if an employee makes purchases using his work computer from a site that sell guns and bomb-making materials and then goes out and uses them? Can the company be held responsible because it didn't take action quickly enough to prevent this employee from using its computers to further his goals?

Moderator: Given the disparate privacy standards throughout the U.S. and around the world, how are you advising clients to establish privacy programs?

Anolik: In this day and age, companies can't afford not to establish privacy programs. That said, there is no such thing as a one-size-fits-all privacy program. There are numerous elements to developing an effective, tailored privacy program. First, companies need to devote time and resources to asking themselves how important privacy is to them. What are the company values? Where does privacy fit in? How important is the company's brand and reputation? Does the company want to be a leader or a follower in the privacy arena? Before the first privacy policy is drafted, a company should really do some corporate soul searching to determine what role privacy will play within its organization.

In addition, hiring a full-time, experienced privacy professional who knows how to frankly assess your current privacy operations shows a significant corporate commitment to taking privacy seriously. That person should know how to lead tough conversations, develop workable policies for your business, educate internally to build awareness of privacy issues, make decisions, and work with many different areas of, and personalities within, the company. Ideally, they also should know the law and have experience with policymaking and public speaking, which can be very helpful. The right privacy professional has an interesting mix of skill sets that they bring to the table.

Gordon: Many U.S. businesses simply don't have the resources to have a full-time privacy officer or staff of people who can focus exclusively on privacy. These businesses still need to address privacy because of the increase in privacy legislation at the state level. For these businesses, the key is to discuss privacy with a knowledgeable consultant or counsel who can identify the most significant

risks to the organization arising out of potential privacy breaches and privacy laws, and at least put in place a lesser privacy program that will protect the organization from the most significant risks.

Wugmeister: What I have also seen work within organizations is a cross-functional and cross-regional privacy council. It's very hard, even if you have an experienced, knowledgeable person in the U.S. implement a privacy policy across a global organization. It is essential to get buy-in from very senior people that this is an important value and obligation of the company on a global basis. Otherwise it will be virtually impossible to get anything done. What has worked effectively for several of my clients is that they have a privacy council or privacy committee that is across businesses and across countries. They are then able to obtain consensus on how to implement a privacy program throughout the organization.

With global databases and the desire to cross-sell and to maximize efficiencies, organizations are centralizing much, much more information, and as a result they are looking for common approaches to the use of information across a global organization.

Lefkowitz: The good news is we are starting to see some convergence in the law and in practice. Breach notification laws in the U.S. are almost to 40 states, probably close to 50 soon. Japan has something similar, and the E.U. may be coming soon. On data retention, where countries have been quite far apart, the E.U. is starting to recognize that not all data must be purged immediately, and the U.S. is starting to see that not all records should be kept forever because of litigation and security concerns. These changes are making it easier for us in-house to suggest paradigms that can work globally for marketing data, for HR data, for sensitive data, and for treatment of systems.

Sharon Anolik is the Privacy Official for Blue Shield of California, where she is responsible for privacy policies and procedures, compliance with privacy regulations, and privacy training for more than 4,500 employees. She is a former Judicial Clerk to the California' Supreme Court, and recently served as a Privacy Specialist for Deloitte & Touche, and Associate General Counsel & Chief Privacy Officer for Ask Jeeves. Ms Anolik is an adjunct law professor at Golden Gate University, teaching cyberlaw and privacy. sharon.anolik@blueshieldca.com

Philip Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., the largest law firm practicing exclusively labor and employment law. He chairs the firm's Privacy Practice Group. Mr Gordon regularly counsels clients on workplace privacy and information security issues. He teaches privacy law as an adjunct professor at the University of Colorado Law School and is co-author of the book HIPAA Privacy for Employers. He is a graduate of Princeton University and N.Y.U. Law School. pgordon@littler.com

Peter M Lefkowitz is Oracle Corporation's Chief Counsel, Privacy & Security. He works with Oracle's security and information technology organizations on company security policies and practice standards, and advises Oracle's outsourcing, support and consulting services business and various internal business groups on privacy and security requirements. Mr Lefkowitz received his under-graduate degree from Yale University and his J.D. from Harvard Law School. He clerked for the Honorable Robert E. Coyle, Chief Judge of the U.S. District Court for the Eastern District of California. peter.lefkowitz@oracle.com

Miriam Wugmeister is a partner in the New York office of Morrison & Foerster and head of the firm's Privacy and Data Security Practice. She regularly counsels clients regarding the collection, use, disclosure and transfer of personal information as organizations seek to comply with U.S. and international data protection laws. Ms Wugmeister received her J.D. from Boston University School of Law, and her B.S. from Brandeis University. She is admitted to practice in California, Connecticut, and New York. mwugmeister@mofo.com