WINSTON & STRAWN LLP

PODCAST

Episode 5: How Do Privacy and Security Laws Affect Employers?

JULY 1, 2019

13:18

We encourage you to subscribe via Apple iTunes or Google.

Audio Transcript

Steve Flores: Welcome to another episode of Winston's Benefits Blast Podcast. I'm Steve Flores, and I'm delighted to be joined today by my colleague, Alessandra Swanson. Alessandra is a former federal regulator with the U.S. Department of Health and Human Services Office of Civil Rights. She now focuses her practice on privacy, marketing, advertising, and intellectual property, and is a member of the firm's Global Privacy & Data Security Task Force. During this episode, we'll be talking about how privacy and security laws affect employers. Alessandra, data privacy and security are topics that are constantly covered in the news. Can you tell us a little bit about what's going on in this space?

Alessandra Swanson: Sure, this is a really interesting time to be a data privacy and security lawyer. Maybe a little less interesting to be on the regulated side of this, but the U.S. is currently undergoing a huge shift in how the privacy and security of personally identifiable information is regulated. Previously as background, it was more of a patchwork of laws that regulated how companies could collect, use, and share certain classes of personal information, so that would include things like GLBA which regulated financial institutions, HIPAA, which regulated health care providers, and health plans, and then, there were a patchwork of state laws, most notably Massachusetts, which regulated the security of personal information that can be used for identity theft purposes, that was named in Social Security Number, name, and driver's license number, things of that nature.

Alessandra Swanson: Now, there's a movement especially among the states to create more of a comprehensive scheme, and because the federal government has not responded to this yet, states are taking matters into their own hands. What's been in the news most recently is California which passed the California Consumer Privacy Act in June 2018, it's set to go into effect in January 2020, and for all the employers out there, it mirrors HIPAA in that it governs a very wide class of personally identifiable information. It's essentially anything that can be identifiable to an individual, or a household, and it introduces a number of individual rights or ways that consumers can control what a company does with their personally identifiable information.

Alessandra Swanson: So, this is very reminiscent of HIPAA, which governs PHI, protected health information. It's essentially anything remotely identifiable that a health care provider or a health plan is holding, and individuals have a lot of rights with respect to accessing, amending and controlling how the healthcare industry can share that information. CCPA is a little bit different because the information that it seeks to govern is information that previously really flew under the radar of other regulations. It could be something as simple as an individual's name, and the fact that they're a customer of a company. That's really going further than U.S. privacy law has gone in the past. Of note to our audience, the laws written arguably applies to employee information, but, it's widely understood that the laws going to be amended to exempt employee information, so it would still govern... if a company holds consumer information or other customer information, but hopefully the laws are geared towards consumers, so it will not impose obligations with respect to employee information.

Alessandra Swanson: That stated there are about 11 other states that are currently contemplating laws that are similar to see CCPA, and the federal government is kicking around potential laws that could partially, or fully preempt state laws on point. At this point, we just have to stay tuned to see what direction we go in.

Steve Flores: Thanks, Alessandra. What does this mean for the privacy and security of employee information? What should employers be on the lookout for?

Alessandra Swanson: One critical area for employers that's part of both these widespread privacy laws like CCPA, and then, other specific state laws, it's the collection of biometric information, which includes retina scans, fingerprints, and handprints. In the employment context, this usually comes up for timekeeping purposes. If you are having your employees clock in and clock out by using a fingerprint scanner, or hand scanner, but it can also arise in other employment situations such as verifying someone's identity if they need to enter a locked cabinet or a locked room.

Alessandra Swanson: Currently Illinois, Washington, and Texas have laws that require certain notice and consent from individuals before this information is collected, and then, there's also some data security requirements that go along with that. Illinois, in particular, has been in the news a lot lately, because its law, The Illinois Biometric Information Privacy Act, has a private right of action for, "Aggrieved individuals, and unkept statutory damages." This year the Illinois Supreme Court had a ruling saying that someone can be aggrieved without suffering any type of damage just because their biometric information was collected absent notice, so that has really opened the floodgates of litigation.

Alessandra Swanson: And, because this comes up in the context of timekeeping, and other employment-related issues, a lot of the plaintiffs are ex-employees or angry employees. It's something to keep their eye on for sure. Another area that's not new, but still important is HIPAA compliance. For those employers with self-insured health plans, HIPAA poses obligations to create fulsome compliance programs with respect to the privacy and security of protected health information. These compliance programs include things like written policies, and procedures to implement the requirements of the three prongs of HIPAA, the privacy, the security, and the breach notification rules.

Alessandra Swanson: It includes the requirement to address the 50 plus safeguard requirements of the security rule, to conduct a security risk analysis, create an incident response plan, and to enter into business associate agreements. Again, HIPAA, compared to some of the other privacy laws we've been talking about HIPAA's kind of an old man privacy law. It's been around for a long time, but it does still impose obligations, and it is enforced by HHS OCR where I used to work before coming to Winston.

Steve Flores: Alessandra, it seems like I hear about a new breach almost every single day. Again, can I ask you what should employers be on the lookout for in terms of data security?

Alessandra Swanson: Sure. In terms of data security with employers, I think a top issue just based on what I'm seeing in my practice, it's phishing schemes, and how often employees can fall victim to them. Phishing schemes are when you get an email, it looks legit. Maybe the email address is one letter off, and the bad actor who sends the email either request that you send them information, or they trick the user into clicking on a link, and they enter your system that way, or they can request your user credentials, something like that, and they enter your system, and they're on the lookout for any valuable information.

Alessandra Swanson: The bad actors who run these phishing scenes, they're incredibly sophisticated. You have to pay very close attention. They'll even mimic sending emails from company executives, from a company's IT team, so it's really a matter of educating employees again, and again, and again, reminding them that this is a threat, and then, testing them on that. A lot of organizations will send fake phishing emails, and they'll kind of catch their employees, and then, implementing effective security measures, which includes spam filters, so these emails don't hit your system.

Alessandra Swanson: And also, a lot of people when there's an external email that comes in, there's an automatic header put on the email saying that it's external, so something to alert your employees to take care with looking at the email. Another issue that comes up a lot, it's the security of end user devices. That would be things like smartphones that your employees are using if they can access company information through them. Also, laptops, flash drives, things of that nature. The number one way to prevent a breach is to encrypt these devices, and to educate your employees that they shouldn't be saving information outside of your network, and your database, that they should protect their devices when they're off company grounds, and things like that.

Steve Flores: This seems like a lot to manage, and here you talked a little bit about how an employer can address phishing threats and the security of end user devices. What are some other things that employers can do to protect themselves?

Alessandra Swanson: Sure, it is a lot to manage. It's a lot to think about, but the first thing an employer needs to do is to data map. They need to understand where their sensitive information, their employee personal information, HIPAA protected information, biometric information, they need to know where that "lives" in their organization in order to protect it. They need to know what their employees are doing with the information. When I say data mapping, I mean, looking at how the information comes into your organization, where it resides on your IT servers, and then, how it exits, so any vendors that you're sharing it with, any other third parties, any removable devices that it may travel to, things like that.

Alessandra Swanson: Once, you can wrap your mind around what's going on with your data, then you can sit down, and make a plan to best protect it. Going hand in hand with that is conducting regular security risk assessments to understand any vulnerabilities to your data, penetration testing, to make sure that bad actors malware can't enter your network, and then, kind of another prong that is related is looking at your commercial contracts, and thinking about your relationships with your vendors. What I mean there is, thinking about who has access to your employee information, and your sensitive information, and then, actually sitting down, making sure that you have all necessary contracts in place.

Alessandra Swanson: For example, if you have a HIPAA covered health plan, making sure that there are no gaps in your business associate agreements, that you have agreements in place with every vendor that's receiving your PHI, and then, just generally looking at your contracts, seeing what kind of data security promises you have in there. Is it that the contract is silent on how your vendor's going to protect your data? Does it say that they have to use reasonable safeguards? Is there a two-page addendum outlining the type of security safeguards they need to have in place? Depending on how sensitive your information is, the latter is usually the best practice to make sure that they are effectively protecting your data.

Alessandra Swanson: The contract terms are important, because in the event that your vendor has a security incident or a breach, number one, you want to be informed about it, and number two, you want to be able to point to something in the agreement that will afford you some recourse, because you will definitely incur expenses on your own end, investigating, providing notification, working with legal counsel, working with an IT vendor. You want to make sure that your contract has all of those terms, and if not, it would be worth going to your vendor and asking to engage in a new agreement.

Steve Flores: Thank you all Alessandra for sharing your insights about how privacy and security laws affect employers. Thank you to our listeners for listening to another edition of Winston's Benefits Blast Podcast. You can subscribe to the Benefits Blast Podcast via Apple iTunes, or Google Play, or by visiting our website at www.winston.com.

Speaker

Alessandra Swanson

Related Locations

Chicago

Related Topics

Podcast | Health & Welfare | Data Breach | Biometrics

Related Capabilities

Privacy & Data Security | Employee Benefits & Executive Compensation | Labor & Employment | Compliance Programs | Health Care | Technology, Media & Telecommunications

Related Regions

North America

Related Professionals

Alessandra Swanson