Legaltech news

The Biggest Cyber Challenge? A Former Big Law Co-Chair Says It's People

It isn't the actions of a hacker companies should fear the most, but instead an employee's or contractor's mishaps, warned former Greenberg Traurig shareholder Francoise Gilbert.

By Victoria Hudgins | August 13, 2019

Francoise Gilbert, CEO, DataMinding. Courtesy photo.

Earlier this month, Francoise Gilbert left her post as shareholder and co-chair of Greenberg Traurig's data, privacy and cybersecurity practice group. But while she wanted a break from Big Law's billable hours, she hasn't entirely stepped away from her practice: Earlier this month, Gilbert officially launched legal consulting and cybersecurity consulting firm DataMinding, where she works as CEO.

In a chat with Legaltech News, Gilbert discussed her new move, the top cybersecurity challenges her clients face, and how organizations are trying to shape the evolving data privacy landscape. This interview has been edited for clarity and brevity.

Legaltech News: What have you been up to since leaving Greenberg Traurig?

Francoise Gilbert: Many things. I have started this new company, which is going to be a mixture of legal services and consulting services where I will continue working with a small number of clients. And I have other activities: working on version two of my book [2009's "Global Privacy and Security Law"], working for a large trade association as their global privacy ambassador, and if I have some time I'll continue my research in privacy [and] cybersecurity.

Do you believe some companies think they aren't affected by privacy laws?

Those that come to me have realized they have an obligation to comply with laws, but there are a number of companies that do not understand the requirements or need to be educated on those requirements. Or they think the requirements don't apply to them. Frequently, when I meet a company I'll say, 'What type of personal data are you collecting?' and they'll say, 'No, we don't.' We need to

help them understand what personal information is. Even with that, the definition of personal information has changed so much, we are chasing a moving target.

What is the most common cybersecurity challenge for companies?

To me, the number one challenge is people. As we've seen for example in the most recent security breaches, many of the errors and breaches and mishaps are caused by people, so companies need to do much more to train their employees, monitor what they do and increase their awareness. Without that, everything else fails.

What are some of the most important cybersecurity regulations for your clients?

They are not regulations per se but there are efforts by a number of organizations to create some consistency amongst the laws so there is an easier interchange of data between countries. For example, the OECD [Organisation for Economic Co-operation and Development] back in the 1980's then later in 2013 created data protection principles and security principles to be adopted and interpreted by countries throughout the world. You have efforts by the European Union to create laws that apply in 28 countries. There are the efforts of the APEC [Asia-Pacific Economic Cooperation] in the Asia-Pacific region to create the common privacy framework so that countries are able to interact and integrate with each other.

Are there any state-level cybersecurity or data privacy laws that have your attention?

Plenty. One I would cite is biometric laws. Illinois is one of the drivers in the collection of biometric information and we've seen a number of cases there. We've seen a number of municipalities as you've mentioned (https://www.law.com/legaltechnews/2019/07/22/compliance-complexities-grows-as-more-cities-ban-facial-recognition-tech/) that also want to curb the use of facial recognition technology, [which is being] principally conducted by the police authority with a different goal, but these are very significant laws because biometrics is a type of information that is with a person forever. It doesn't change. It's a recognition that this is a highly sensitive type of information and it should not be collected without good reasons and good purposes.

Other laws of interest are related to the CCPA [California Consumer Privacy Act]. New York for example is working on a law that would be similar to the CCPA.

I saw on the DataMinding website that you mentioned smart cities. Are there cybersecurity issues related to them?

Yes, I'm passionate about smart cities because it's where the future is for each of us as citizens, but the interconnection of so many computer systems, sensors and cameras under one hub is by itself a huge privacy and cybersecurity issue. We need to be aware of the high risks of privacy invasion and privacy security risks. We've seen a number of problems, one example that comes to mind is Atlanta that was the victim of ransomware. There are numerous other cities (https://www.law.com/legaltechnews/2019/07/11/5-municipalities-sacked-by-cybersecurity-attacks/) that have been the victim of cyberattacks.