LAW & CYBER SECURITY

EXPERT OPINIONS ON HOT TOPICS

Interviews conducted by:
Katie Haug, Kevin Pouche, & Kevin West

During the RSA conference, we interviewed two lawyers who focus much of their work on cyber security. By interviewing non-CISOs, we are able to understand a different perspective on key industry trends and concerns.

We first spoke with Stephen Wu, Shareholder, Silicon Valley Law Group.

As a seasoned lawyer with a focus on information security, in what instances do you interact directly with CISOs?

We're working very much hand in glove with each other. Some CISOs are spending a lot of time with contract drafting and negotiation. The day-to-day work of contract review and negotiation calls takes them away from their core function of security management. Consequently, they have to hire people to help them. As a lawyer, I help them by taking on some of the burden of negotiating security agreements or security exhibits to larger contracts. We will take turns reviewing contracts and negotiating deal points on customer and vendor calls. From time to time, I also work with CISOs on meeting compliance requirements and to support security audits and certifications.

I recommend that CISOs hire people to interface with lawyers like me to further lighten the CISO's workload. Those people need to have skills that bridge between law and security. So, if you hired a security person who has no legal training, then that person must be trained in key legal topics. If you hire a lawyer who doesn't know information security, it's not going to work because then he or she doesn't know the security environment. Relying on checklists is not enough. Team members need to be able to bridge between law and security. I think there's an opportunity for information security professionals who have knowledge of both security and the legal aspects of contract negotiation.

How does Artificial Intelligence fit into your work?

I work in the areas of transactions, compliance, litigation, liability, investigations, and policies and procedures in AI and robotics as well as information security and privacy. I started in information security and privacy in 1997, but since 2007, I have been trying to incorporate more AI and robotics matters into my practice. My work in the area of automated transportation is a good example.

With transactions, I help AI and robotics companies sell their products and services. I advise clients on how to comply with various laws that apply to AI and robotics, such as GDPR and California's new bot disclosure law. With litigation and liability risk management, I counsel clients on taking steps today to win lawsuits tomorrow for products that you haven't even finished yet. It is important to build in safety into the products and services now, consider ways to eliminate possible bias, and think about legal issues that would come up in the future. My law firm also defends companies when they are sued. Our lawyers investigate accidents and data breaches and prepare for future legal proceedings. Finally, we help establish policies and procedures to govern AI and robotics development, procurement, and operation, similar to the privacy and security policies I write for clients in my data protection practice.

We also spoke with Adriana Sanford, International TV Commentator, Strategic International Consultant, AND Cyber Security Expert.

Adriana shares her expertise on the California Consumer Privacy Act. She says:

Much like the GDPR, the CCPA is expected to have far-reaching impact on businesses on a global scale. In contrast, however, while the GDPR applies to all EU citizens regardless of where they reside in Europe, the CCPA only protects California residents. The CCPA is expected to affect 1 in 8 Americans, but only while they reside in the state. The territorial protection of the GDPR is much broader; GDPR follows the EU citizen anywhere in Europe.

Although the law will not be effective January 1, 2020 and more clarification is coming, businesses should not take a wait-and-see-approach. Internal policies may need to

HEAR FROM STEPHEN WU AND ADRIANA SANFORD ON:

CISOs and Cyber Law, Artificial Intelligence, California Consumer Privacy Act, and More

be amended as compliance with GDPR and other current privacy laws may not adequately prepare some companies from the wide-ranging impacts of this new law. Businesses will need time to properly analyze and adjust contracts with service providers, conduct or review data mapping, as well as ensure that sufficient processes and resources are in place to adequately respond in a timely manner to consumer requests for access or deletion of their personal information. Personal information includes more information than what is required under GDPR. In addition to various types of internet activity ranging from searching and browsing to histories and tendencies, CCPA also includes inferences and attitudes, as well as interactions with online advertisements. Businesses need to start thinking about how CCPA requirements may impact their business operations.

CCPA will create a de-facto baseline standard for the US on data privacy controls and processes. California is the world's fifth largest economy and science and technology comprises a big sector of that economy. This may allow for more predictability of results in the future, particularly if Congress takes the lead or if other states begin to adopt a variation thereof.

Last year, many companies became consumed with GDPR and ensuring security and privacy were aligned. Businesses now need to focus their international efforts on a more territorial scale. They need to take a "glocal" approach to stay compliant. This may present a challenge for some businesses that have traditionally relied on a more simplistic approach.

The complex and rapidly evolving set of global data privacy regulations in the United States and foreign territories have radically changed the way that companies throughout the world handle data and their business operations. Within our changing global security landscape, several new foreign laws have an extraterritorial reach. There is a significant degree of frustration when demands from multiple regulators from different jurisdictions conflict with one another, particularly when there are hefty fines and potential liabilities for corporate executives, including criminal liability. Executives constantly need to re-shuffle their priorities.

I believe we need to be considerably more proactive in providing the private sector with guidance and direction when the laws conflict. The traditional 'reactive approach' leaves executives and general counsel exposed. There is currently is a lack of uniformity and predictability on the international level when laws do not mesh with one another. This scenario places multinationals and their employees in a terrible predicament. This has to change, as it is not fair to the executives or the businesses. The private sector has a significant challenge in this global space.