Lessons from the trenches at Philadelphia privacy summit

(April 26, 2019) - Law firm Fox Rothschild hosted its second annual privacy summit April 24 in Philadelphia, where privacy professionals with diverse backgrounds discussed the importance of knowing the location of their organization's data, training on information security, and applying lessons from regulatory enforcement and litigation actions.

"Companies must think about data as both an asset and a liability, but most significantly, as a company responsibility," said Elizabeth Litten, a Fox Rothschild partner who moderated the summit's first panel on data collection, usage and compliance issues.

Litten is Fox Rothschild's privacy and security officer under the Health Insurance Portability and Accountability Act of 1996.

She co-chairs the firm's privacy and data security practice with Mark McCreary, Fox Rothschild's chief privacy officer.

Both McCreary and Litten said Fox Rothschild started its privacy summit to raise awareness about the privacy and information security issues organizations need to address.

"These are also topics that often end up being addressed in a reactive manner, often after something bad has happened," said McCreary, a certified information privacy professional.

Rather than keep the status quo, Fox Rothschild took proactive steps to create a free, collegial forum to discuss these complex and important topics with experts and those who simply seek more awareness, he said.

"Hearing from professionals whose job is specifically to address these issues, supplemented with lawyers who advise those professionals, resonates with in-house counsel and C-suite executives alike," McCreary noted.

Litten echoed and added to McCreary's thoughts.

"Another reason for hosting these privacy summits is to encourage companies of various types (and subject to various laws) and people with various roles within these companies to share ideas and concerns that transcend particular industries and roles," she said. "A hospital system's suggestions for data minimization or access control may help a retail chain, for example."

Panelists at this year's summit included in-house attorneys, customer experience directors, and privacy and operations officers from state agencies, health care systems, financial news organizations and technology companies.

Despite the participants' diverse industries, one of the common themes that emerged throughout the day was that the work of privacy and information security professionals at any organization is never over.

This point especially came across during the panel on monetization of consumer data that Fox Rothschild partner Odia Kagan moderated.

The changing legal landscape, the fast-paced deployment of new technologies and potential innovative uses for collected data all contribute to this constant workflow, the panelists said.

The speakers also discussed the European Union's General Data Protection Regulation, which took effect a year ago. The GDPR imposes privacy and data security obligations on businesses and service providers that operate in the EU or handle personal data for EU residents.

"GDPR enforcement is just getting started and is a real issue both because of fines and because of other mechanisms in the regulator's toolbox, like prohibiting further processing of the data until you are compliant," Kagan said. "On this side of the pond, CCPA [the California Consumer Privacy Act] and other burgeoning state laws are something to think about starting right now."

U.S.-based service providers that process consumer data may have thought they did not have to comply with the new EU regulation, but now they now face a new privacy law in California and potentially other U.S. states, she said.

"The preparation needed for compliance is time-consuming and there is a lot of work to do even for companies that have undergone a considerable amount of GDPR compliance work," Kagan said.

Horror stories seem to be an effective tool to reiterate the importance of privacy and data security to employees and C-suite executives who may be reluctant to spend the time or resources addressing these issues.

To drive home this point for attorneys and law firms, McCreary's presentation on information security included a January 2019 headline about how an associate at Dentons Canada transferred $2.5 million from the law firm's trust account to fraudsters in a business email scam.

Savvy recipients can spot many tricks by pausing to check email address spellings and formats or hovering over URLs to see where a link really intends to go, McCreary said. He added that typos, unusual characters or subject lines, unexpected reply-to email addresses, and grammatical errors should all raise red flags.

He reminded the audience that good security practices apply in both professional and personal settings.

By Melissa J. Sachs

End of Document