Insights: Publications

3 Key Takeaways | Privacy in a Flash: Keeping Up with Rapid Changes in State Laws

March 3, 2025

Written by **John M. Brigagliano**

Kilpatrick's **John Brigagliano** recently spoke at the Association of Corporate Counsel (ACC) DFW Annual In-House Symposium in Frisco, Texas. John spoke on the topic of "**Privacy in a Flash: Keeping Up with Rapid Changes in State Laws**" where he addressed how in-house counsel can navigate the rapidly shifting landscape in state privacy regulation while reducing compliance costs, enabling business objectives, and minimizing legal risks.

Key takeaways from John's presentation include:

1. Shifting privacy risk in vendor contracts requires redrafting or negotiating form language. First, standard provisions that require mutual compliance insufficiently protect customers. Customers with sufficient leverage should instead require vendors to not cause the customer to violate applicable privacy laws. Second, damages arising from security incidents aren't captured through breach notice costs. Customers should exclude such damages from liability limits and caps. Participants in the crowd generally considered "supercaps" on security incident damages of $5 million to $20 million to provide sufficient coverage (depending on the nature of their business).

2. Don't take a myopic approach to privacy compliance. Legal media and third-party vendors tend to heavily focus on newly passed state consumer privacy laws as a primary driver of privacy compliance. That overstates the risks presented by those laws for several reasons. For example, those laws are largely interoperable. Any newly passed law therefore presents, at most, marginal new compliance requirements. Those consumer privacy laws also lack private rights of action and contain many exceptions.

3. AI training presents unique privacy risks. Companies using personal data to train AI products must consider privacy alongside other legal risks. We discussed several challenges to doing so. Establishing sufficient rights in such personal data can be difficult as upstream third-party contracts and prior notices delivered to consumers may limit the company's use of personal data. In terms of privacy operations, companies should evaluate whether their privacy rights operations (i.e., data governance) and controller-processor designations account for any use of personal data for AI training.

For more information, please contact:
John Brigagliano, jbrigagliano@ktslaw.com

Related People

John M. Brigagliano

t 404.815.6135

jbrigagliano@ktslaw.com