Kilpatrick

Insights: Perspectives

5 Key Takeaways | Navigating the New Data Privacy Landscape

May 18, 2023

Written by **Meghan K. Farmer** and **Anthony D. Glosson**

KILPATRICK TOWNSEND

5 KEY TAKEAWAYS

Navigating the New Data Privacy Landscape

Kilpatrick Townsend's Meghan Farmer, Alex Borovsky, Jennie Cunningham, and Zain Haq recently presented "Navigating the New Data Privacy Landscape" at an event sponsored by the Association of Corporate Counsel Nation Capital Region Chapter. Blue Cross Blue Shield Association's Associate General Counsel for Privacy Devi Mehta participated in the presentation.

Companies and their in-house counsel have been preparing for and navigating a significant shift in the data privacy regulatory landscape. With new laws going into effect in multiple states, and others expected to follow, in-house counsel need to understand the various statutes and implications in order to build strategic data privacy programs that best meet the needs of their businesses. The discussion offered practical guidance on compliance with the comprehensive U.S. data privacy laws with case studies, as well as recent trends in data privacy litigation.

Kilpatrick Townsend offers five key takeaways from the presentation:

1

Determine which data privacy laws apply to your organization. Not all organizations are going to be subject to all the comprehensive U.S. state data privacy laws. Factors for determining applicability include: (a) your organization's annual revenue; (b) the number of consumers for which the organization controls or processes personal data; and (c) if your organization derives revenue from the "sale" or "sharing" of personal data. In addition, it is important to determine whether your organization can rely on any exemptions to the laws. Each law has different applicability thresholds and exemptions, so it is important to perform this step on a state-by-state basis.

2

Conduct strategic data mapping in order to determine and understand: (a) the source of your organization's personal data; (b) the type of personal data your organization processes; (c) how your organization is using personal data; (d) which third parties have access to personal data; and (e) your organization's role under the comprehensive U.S. state data privacy laws. Data mapping may help your organization comply with data minimization concepts under some of the comprehensive U.S. state privacy laws, but it may also help your organization to understand its other obligations under these laws. For example, through the data mapping process, your organization can determine whether it processes sensitive personal data that would be subject to opt-in or opt-out consent requirements.

3

Consider your organization's requirements and approach with respect to employee and B2B data. Currently, the comprehensive U.S. state privacy laws exempt individuals acting in an employment or commercial context from the definition of a consumer, except for the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA"). Therefore, if your organization is subject to the CCPA, consider providing a separate privacy notice to your California employees, evaluate how your current data subject request process applies to your California employees, and determine whether any of your employment-related contacts need required language under the CCPA.

Draft a compliant privacy notice for your consumers. Every state with a comprehensive data privacy law requires a privacy notice, and each law has varying requirements for what information needs to be included in the notice. Updating your privacy notice to comply with the new state requirements should be a top priority for every organization

comply with the new state requirements should be a top priority for every organization. Your organization's outward data privacy disclosures, particularly around the "sale" of data, and the ability to opt-out of "sale", has been a focus area for enforcement, and is expected to be moving forward. Some similarities between state law requirements for a privacy notice include: (a) describing the categories of personal data processed; (b) the purposes for processing; (c) categories of third parties to whom the information is "sold", "shared", or disclosed; (d) explaining the consumers' rights and how they can exercise their rights; and (e) providing contact information for the organization. To comply with the CCPA's unique requirements, many organizations are including a California-specific section in their privacy notice.

4

5

Keep an eye on national trends in data privacy related litigation. Two areas currently seeing an uptick are: (a) lawsuits filed pursuant to state wiretap laws and (b) lawsuits filed under the Video Privacy Protection Act ("VPPA"). If your website uses session replay or other technology to capture a website user's communication or interaction with a website without the user's consent, you may be at risk for wiretap lawsuit. Recent lawsuits under VPPA have focused on organizations with a website with video viewing capabilities deploying tracking pixels that collect and disclose information to third parties about a website user watching these videos. Being informed of the tracking technologies your organization utilizes and staying up to date on decisions in these areas will help your organization mitigate risk.

For more information, please contact Meghan Farmer:
mfarmer@kilpatricktownsend.com

www.kilpatricktownsend.com

Related People

Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com

Anthony D. Glosson

t 202.508.5842

tglosson@ktslaw.com