KILPATRICK TOWNSEND

5 KEY TAKEAWAYS

US State Privacy Law

Kilpatrick Townsend's John Brigagliano recently participated in the **"US State Privacy Law"** panel at the 37th Annual Privacy & Technology Law Forum. Mr. Brigagliano moderated the discussion with **Jason Loring** (Vialto Global Head of Privacy and Data Protection) and **Kaeley Brown** (Snap Inc. Privacy Counsel). Thought leaders at the forum discussed topics including ransomware, cryptocurrency litigation & trends, data transfers, privacy & cybersecurity considerations in M&A, and ethics. Kilpatrick Townsend's Amanda Witt co-chaired the forum with **Julia Neighbors** (State Bar of Georgia).

Mr. Brigagliano's five key takeaways from the panel include:

1

Old anti-wiretap laws are being applied to new technology in a way that creates a new risk vector for companies. Plaintiffs allege that certain website tools, such as session replay technologies and chat bots, surreptitiously capture or record "communication." Plaintiffs allege that activity violates anti-wiretap laws in states that require consent from all parties before a conversation may be lawfully recorded. Such wiretap laws are an attractive basis for class actions because plaintiffs (i) don't need to prove harm, (ii) the laws don't protect only consumers, and (iii) the laws don't contain industry exclusions. In house counsel should protect their businesses by staying on top of what tools the business launches on its websites, deploying consents when possible, and adding arbitration provisions and class action waivers to website terms of use.

The legal risk of using biometric technology in Illinois is increasing, and that risk may soon spread elsewhere. Illinois currently has a "biometric" privacy law that has generated thousands of class actions in recent years. The law provides statutory damages to plaintiffs for even technical violations. A recent decision from the Illinois Supreme Court enhances that risk by clarifying that each time a biometric is scanned, a separate violation of the law occurs. Despite the litigation nightmare in Illinois, several other US states are considering laws similar to Illinois's statue.

2

3

Consumer-focused laws don't apply neatly to "HR" and "B2B" data. California's comprehensive privacy law, the California Consumer Privacy Act ("CCPA") excluded from its scope the personal information of individuals acting as an employee (or similar role) or on behalf of a business. That exclusion expired January 1, 2023, and the law's application to such data is awkward. First, the CCPA was written to apply to consumers, and so the law and its implementing regulations often contemplate a consumer receiving products or services from a business rather than acting as the business's employee. Second, California already has a legal code governing the employer-employee relationship that counsel must consider alongside the CCPA. Counsel may have to rely on creative lawyering to reach workable compliance positions.

Comprehensive laws are diverging into two models—California and everywhere else. The comprehensive consumer privacy laws that states have adopted are mostly consistent—except for California. California's law differs from the rest in, among other ways, terminology, enforcement cure periods, and consumer rights over sensitive data. The panel discussed that working towards consistency among laws is a way for state lawmakers to protect consumers while minimizing compliance costs for businesses.

4

5

Communicating the rapidly changing landscape to leadership is difficult, but critical. Privacy lawyers must often keep executives or boards of directors apprised of how the business's privacy compliance program protects the company from legal and regulatory risk. That communication is challenging since, among other reasons, legal risks and compliance requirements rapidly change. The panelists advised lawyers facing such a challenge to (i) proactively describe how the privacy team protects the business, (ii) remain honest with leadership that some uncertainty exists in this area, and (iii) describe the business's privacy stance as a part of the business's value proposition to its customers.

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