



Alerts

What's Keeping Corporate Directors & Officers Up at Night: Accelerating Privacy Regulation

January 28, 2020

Hinshaw Alert

The range of issues confronting today's business leaders is enlarging at breakneck speed. Emerging concerns, such as geopolitical unrest, corporate governance mishaps, and climate risks, can have significant impacts on strategic planning, business operations, and revenue. Increased interconnectivity and disruptive technologies create opportunities, but frequently have unforeseen consequences. In addition to adverse financial and operational impacts, a single misstep in managing these complex areas can damage corporate reputations almost overnight.

Against this complicated and varied backdrop, however, one emerging risk has been identified as the key issue keeping business leaders up at night. According to a recent [survey](#) by the Gartner research firm, the acceleration of privacy regulation is the top concern of executives across all industries.

Liability challenges created by the evolving privacy regulatory landscape

Privacy was once thought of as an obscure concern impacting only certain specialized and international organizations. No more. From the EU's General Data Protection Regulation (GDPR) to the California Consumer Privacy Act (CCPA), new privacy requirements are cropping up around the globe. The reach of today's privacy laws and regulations is long, capturing companies in every industry vertical and across borders. Privacy mandates now apply to broad categories of previously unregulated information that modern businesses today routinely collect and store.

Simply keeping pace with new privacy mandates and understanding their impact on business operations and budgets is challenging. Non-compliance, however, is not an advisable option. Recent laws can provide for hefty regulatory fines, injunctions, and statutory damages, even in the absence of a data breach. Attorneys general are empowered to bring enforcement actions, and as plaintiffs' class action lawyers can attest, some laws contain a private right of action, expressly permitting consumers to bring lawsuits for privacy violations.

The stakes associated with getting privacy right now clearly extend to the boardroom. Privacy-driven lawsuits against directors and officers are on the rise. Plaintiffs have accused boards of failing to exercise their duty to oversee

Attorneys

Steven M. Puiszis

Service Areas

Directors & Officers Liability



privacy and cyber risks in connection with costly data breach events. Boards also have been sued for failure to appropriately consider the impact of privacy compliance on business operations and for failing to accurately disclose the cost of compliance in their public filings. Directors and corporate officers have been removed from their jobs. Some have been grilled before Congress. Regulators, in addition to imposing massive fines, have required companies to establish board-level privacy committees, create privacy programs, designate privacy compliance officers, improve board reporting, obtain regular third-party privacy assessments, and more. And some regulations, such as the [New York State Department of Financial Services Cybersecurity Regulation](#), expressly mandate board oversight.

As with every material risk a company faces, corporate boards have a duty to oversee compliance and monitor privacy exposures. This requires the establishment of appropriate reporting systems and procedures that enable the board to discharge its oversight responsibilities. That oversight should extend beyond mere compliance to the establishment of information governance policies that can drive down the [cost of compliance](#) and streamline business operations. Undertaking good faith oversight efforts minimizes the risk of noncompliance in the first instance and provides protection for the company and the board if something does go wrong.