State-Level Actors on the Frontlines of U.S. Cybersecurity and Data Privacy Regulation and Enforcement

by John F. Savarese, Marshall L. Miller, and Jeohn Salone Favors

While the General Data Protection Regulation (GDPR) significantly expanded the powers of European national data protection authorities in 2018, legislative and enforcement developments in the United States over the last year showcased the growing role and importance of state attorneys general and other state regulators in the realm of cybersecurity and data privacy.

In 2018, California passed a data privacy law akin to the GDPR and enacted legislation addressing internet-based bot activity and security of devices connected to the Internet of Things. With passage of legislation in Alabama in March 2018, all 50 states now have data breach notification laws, with requirements as to notification content, timing, and recipients varying across jurisdictions. And prescriptive cybersecurity regulations promulgated by New York State's Department of Financial Services continued to take effect in rolling fashion. Absent preemptive legislation at the federal level, where proposals are stalled in Congress, we can expect data protection and privacy laws and regulations to proliferate at the state level, as state legislatures and regulators vie for the mantle of lead cybersecurity enforcer.

In connection with many of last year's most high-profile data breaches, state attorneys general took the lead in pursuing enforcement actions. In the wake of Marriott's announcement of a breach of its reservation systems, exposing the personal data of up to 500 million customers, multiple state attorneys general announced the opening of investigations. In a first-of-its-kind state enforcement action under the federal Health Insurance Portability and Accountability Act (HIPAA), the attorneys general of 12 states joined forces to sue an Indiana-based medical records company for failing to

adequately safeguard patient data and timely disclose a breach that compromised the medical records of nearly four million individuals. Coordinated, multi-state data breach actions have become routine fare for state attorneys general, and the use of HIPAA, a federal statute typically enforced by the U.S. Department of Health and Human Services, illustrates the increasing appetite of state-level authorities to engage in enforcement action where federal authorities opt not to act.

These developments send a strong signal that the consequence of federal inaction in this field is not a continuance of the *status quo*, but a ceding of leadership to state legislatures and enforcement authorities. If what's past is prologue, these trends will position state-level actors to exert outsized influence in the cybersecurity and data privacy space in 2019 and beyond, leaving companies to navigate an increasingly complex terrain marked by varying state laws and regulations, data protection and privacy standards, best practices, and industry and customer expectations. From a practical perspective, these developments should serve as a reminder to corporate leaders of the importance of monitoring statutory and regulatory developments at the state level to anticipate future compliance challenges and address enforcement risks.

John F. Savarese is a partner, **Marshall L. Miller** is of counsel and **Jeohn Salone Favors** is an associate at Wachtell, Lipton, Rosen & Katz.

Disclaimer

This entry was posted in Compliance, Cybercrime & Cybersecurity, Data Privacy and tagged Jeohn Salone Favors, John F. Savarese, Marshall L. Miller on February 8, 2019 [https://wp.nyu.edu/compliance_enforcement/2019/02/08/state-level-actors-on-the-frontlines-of-u-s-cybersecurity-and-data-privacy-regulation-and-enforcement/] by Allison Caffarone.