wiley

NEWSLETTER

Mapping a Privacy Path - Liability and Enforcement Recommendations for States

U.S. CHAMBER INSTITUTE FOR LEGAL REFORM
February 2020

Privacy in Focus®

Originally published December 2019. Reprinted by permission, instituteforlegalreform.com, February 2020, Copyright 2019, U.S. Chamber Institute for Legal Reform.

Executive Summary

For consumers to reap the benefits of data-driven innovation, it is important that they can trust that their personal information is being protected. There is clearly a need for a unified national data privacy framework; but, to date, the U.S. Congress has not yet acted.

Meanwhile, states are not waiting on the federal government. State legislators across the country are considering and adopting laws. "Consumer data privacy legislation was introduced or considered in more than half the states in 2019, a substantial increase compared to previous years." A piecemeal approach is not ideal. It creates a confusing patchwork of laws and it increases compliance costs. Worse, it expands the risk of litigation and class actions that will enrich lawyers without benefiting consumers.

What Should State Policymakers Do?

The best approach to comprehensive privacy legislation is a unified federal privacy regime. But in the meantime, recognizing that states may be constrained to act, there are a number of interim solutions for state policymakers. These solutions are not focused on the substantive policy questions at the heart of the privacy and security debates. Instead, these solutions offer commonsense, procedural

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
State Privacy Laws

protections that will help to stem the tide of the state laws that risk "opening the door for opportunistic plaintiffs' lawyers to seek large settlements, even when there is no apparent harm." Each recommendation serves an important function to limit unintended consequences of state privacy and security laws by preventing unnecessary litigation.

The Policy Recommendations

Recommendation 1: Preclude Private Rights of Action
State privacy and security legislation should not include private rights of action—which provide no consumer protection benefits, impose heavy costs on legitimate businesses, and deter innovation.

Recommendation 2: Include Notice and Cure Periods
State privacy and security laws should ensure that covered organizations receive notice of alleged violations, as well as a reasonable opportunity to "cure" alleged violations, before they are subject to an enforcement action or litigation.

Recommendation 3: Offer Safe Harbors
State privacy and security legislation should include reasonable safe harbors for compliance.

Recommendation 4: Include Damage and Civil Penalty Caps
State privacy and security legislation should cap any damages or civil penalties for violations.

Recommendation 5: Define Enforcement Actors
State privacy and security legislation should specify that the state attorney general is the exclusive enforcer of state law.

Recommendation 6: Limit Attorneys' Fees
If state privacy or security laws allow private enforcement, they should limit attorneys' fees.

Recommendation 7: Curtail Municipality Litigation
State privacy and security legislation should prohibit enforcement by municipalities.

The complete "Mapping a Privacy Path" guide can be viewed here.