IS AMERICA FINALLY GETTING A NATIONAL DATA PRIVACY LAW?

Date: 7 May 2026

US Policy and Regulatory Alert

By: Marne Marotta, Liam J. Row, Lauren M. Flynn, Scott J. Gelbman, Vivian K. Bridges

A sweeping new federal legislative proposal could reshape how American companies collect, use, and profit from consumer data. Here is what you need to know.

Your compliance team is already toggling between 20+ state privacy laws—one spreadsheet for California, another for Texas, a third for Colorado. Meanwhile, every smartphone app is quietly sharing location data, health metrics, and browsing history with dozens of third parties. For businesses, it is an operational nightmare. For consumers, it is an invisible free-for-all. That may be about to change.

On 21 April 2026, House Republicans released the SECURE Data Act (H.R. 8413) (the Act), the most comprehensive attempt yet to create a national data privacy standard. Paired with the GUARD Financial Data Act (H.R. 8398), which covers financial institutions under the Gramm-Leach-Bliley Act, the two bills aim to eliminate gaps and overlaps in consumer data protection across the entire economy.

WHAT RIGHTS WOULD CONSUMERS GET?

The Act would codify enforceable privacy rights against data controllers—persons that determine the purpose and means of processing personal data (financial institutions subject to the Gramm-Leach-Bliley Act are separately exempt). Consumers would gain the right to access, correct, delete, and port their data, and to opt out of targeted advertising, data sales, and profiling decisions with significant effects.

Controllers would need to respond to verified requests within 45 days. Consumers may submit two free requests per right per year. Controllers would also need to establish an appeals process for denied requests. These are not aspirational principles, they would be enforceable, uniform, nationwide rights.

DATA MINIMIZATION: NO MORE “COLLECT EVERYTHING, FIGURE IT OUT LATER”

Perhaps the most operationally significant provision is data minimization. The Act would limit collection to what is “adequate, relevant, and reasonably necessary in relation to each purpose for which the data is processed as disclosed to the consumer,” curbing excessive collection and unanticipated secondary uses.

The Act would also require affirmative opt-in consent before processing sensitive data—a category that includes data disclosing racial or ethnic origin, religious belief, health diagnosis, sexual orientation, or immigration status; genetic or biometric identifiers; data collected from children or teens; and precise geolocation data. For companies accustomed to opt-out defaults, this would require rethinking consent architecture from the ground up.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Consider a fitness app that collects geolocation and health data: under the Act, it would need opt-in consent before processing, and could not quietly repurpose that data to train an AI model or sell it to a data broker (defined as a controller that derives 50% or more of its revenue from selling data about noncustomers, excluding persons acting solely as processors).

AUTOMATED DECISION-MAKING: WHEN ALGORITHMS MAKE LIFE-ALTERING DECISIONS

One of the most significant provisions targets automated decision-making. Where a controller relies on profiling to make a decision with a legal or similarly significant effect on a consumer—and that decision is made with no human review, involvement, oversight, or intervention—the Act would require disclosure and give consumers the right to opt out.

The covered categories include decisions to deny a consumer a healthcare service, a rental or lease of housing, or an employment opportunity. An employer using AI to screen out applicants, a landlord using algorithmic tenant scoring to deny a lease, or a health insurer using automated claims adjudication to refuse coverage could all be caught. For companies that have quietly integrated AI into high-stakes decisions, this provision may demand the most immediate attention.

ONE STANDARD TO RULE THEM ALL

For many businesses, the most appealing aspect of the bill is federal preemption. The Act would bar any state or political subdivision from prescribing or enforcing any law that "relates to the provisions of" the Act—replacing the current patchwork with a single national standard. A broad coalition of industry groups, including the US Chamber of Commerce and more than 50 other business associations, have endorsed the bill on the basis that a consistent nationwide standard would strengthen trust, give consumers meaningful control over their information, and provide businesses with the certainty needed to innovate and protect data. State attorneys general would retain authority to enforce the federal standard, preserving existing enforcement infrastructure while eliminating the need for 50 separate compliance programs.

The political fault lines are familiar. Industry groups support preemption but resist broad opt-in consent. Consumer advocates resist preemption that would lower existing state protections. Enforcement would rely on the Federal Trade Commission and state attorneys general—no private right of action—a design choice that may draw criticism from consumer advocates while offering comfort to industry. The American Data Privacy and Protection Act (H.R. 8152) stalled over these same disputes in the 117th Congress. Whether the Act can break through remains the central question.

WHAT SHOULD COMPANIES DO NOW?

The legislative landscape is moving quickly. Our team is tracking the SECURE Data Act and the broader wave of AI and technology legislation in real time—translating developments into practical guidance for clients navigating data practices, compliance programs, and regulatory exposure. Whether you need to assess how the bill's provisions apply to your business, shape your organization's position in the legislative process, or get ahead of

©2005-2026 K&L Gates LLP. All Rights Reserved.

compliance requirements before enactment, now is the time to act. Reach out to our team for a targeted compliance readiness assessment, legislative strategy briefing, or gap analysis. Waiting until the ink is dry is a strategy with real costs.

KEY CONTACTS



MARNE MAROTTA
PARTNER

WASHINGTON, DC
+1.202.778.9202
MARNE.MAROTTA@KLGATES.COM



LIAM J. ROW
GOVERNMENT AFFAIRS ANALYST

WASHINGTON, DC
+1.202.778.9250
LIAM.ROW@KLGATES.COM



LAUREN M. FLYNN
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.9051
LAUREN.FLYNN@KLGATES.COM



SCOTT J. GELBMAN
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.9067
SCOTT.GELBMAN@KLGATES.COM



VIVIAN K. BRIDGES
ASSOCIATE

WASHINGTON, DC
+1.202.778.9227
VIVIAN.BRIDGES@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.