HINSHAW

AI Moratorium, Bulk Data Controls, and Enforcement Trends

June 4, 2025 Edition of *Privacy, Cyber, & AI Decoded*

Privacy, Cyber & AI Decoded Alert | 5 min read
Jun 4, 2025

By: Cathy Mulrow-Peattie, Jason J. Oliveri

To help our clients and readers sort through the volume of privacy, cyber, and AI news, we are switching *Privacy, Cyber, & AI Decoded* to a summary format.

In this first edition, we look at a proposed 10-year moratorium on state and local artificial intelligence (AI) regulation, new federal restrictions on bulk sensitive data, recent enforcement actions by the California Privacy Protection Agency, and the high-profile sale of 23andMe's genetic database.

10-Year AI Regulation Moratorium

The U.S. House of Representatives has passed the One Big Beautiful Bill Act (H.R. 1), a broad federal budget bill that includes a 10-year moratorium on new state and local governments from regulating AI. The bill is currently under consideration in the U.S. Senate. The likelihood of its passage is uncertain, and if passed, legal challenges are expected based on state rights and preemption.

- **What the ban covers:** This moratorium blocks all new state or local laws that specifically target AI models, systems, or automated decision-making technologies.
- The moratorium does not eradicate AI compliance but shifts it to other existing technology-neutral legal requirements.
- Massachusetts' and Oregon's Attorney Generals have already issued guidance that existing laws govern AI, such as consumer protection, deceptive trade practices, discrimination, transparency on the use of personal data, or other similar laws.
- **Why is understanding this moratorium important?** It does not eradicate the need for organizations to develop AI governance and ethical approaches, given that existing non-technical laws continue to apply to AI.

Bulk Sensitive Data Law

The new Trump Administration has given companies some additional time beyond its April 8, 2025, effective date to comply with the Bulk Sensitive Data Law.

- **What does the law entail?** Under this law, the U.S. federal government is restricting access to certain Bulk Sensitive Data of U.S. citizens from foreign adversaries in China, Russia, Cuba, Venezuela, Iran, and North Korea.
- The term "foreign adversaries" includes vendors and investments owned by persons from these countries. Bulk personal data includes biometric, humanomic, health, financial, certain identification data, and geolocation data, as well as data linked to current or former U.S. government employees or contractors in certain bulk level quantities. Bulk quantities vary by data type.
- **U.S. individuals and entities should "know their data," according the Department of Justice (DOJ),** including the kind and volume of data collected or maintained concerning U.S. persons; how their company uses this data, whether they engage in covered data transactions with covered persons or countries of concern; and how such data is marketed. The DOJ expects a road to compliance to include contractual clauses in vendor contracts for non-covered foreign persons, including due diligence and monitoring compliance.
- **Why is this regulation important?** From a risk standpoint, there are potential criminal and civil penalties for violating the act, including up to 10 years in prison and a $1M fine. Given that this is a national security regulation, we expect there will be enforcement of this regulation, especially given the current political environment.

CPPA Data Broker Cases

The California Privacy Protection Agency (CPPA) entered a settlement agreement with Background Alert, Inc. and National Public Data, two data brokers who allegedly violated the Delete Act by failing to register and pay the required annual fee.

- **Background Alert Allegations:** The CPPA alleged that Background Alert engaged in data broker practices by creating and selling consumer profiles using patterns and inferences from public records. The agency determined these activities constituted the processing of personal information under California law. The settlement required the company either to suspend data broker operations for three years or to pay a $50,000 fine.
- **National Public Data Allegations:** The CPPA alleged that National Public Data, a Florida-based data broker, pay a $46,000 fine for failing to register and pay an annual fee as required by the Delete Act. National Public Data made headlines last year after a data breach at the company reportedly exposed 2.9 billion records, including names and Social Security Numbers.
- **Why is this important?** The CPPA is actively enforcing its data broker registration requirements, and failure to register could lead to deeper investigations and severe penalties, such as ceasing operations.

CCPA Enforcement Cases

On May 6, 2025, the CPPA announced its second non-data broker enforcement action, requiring a national retailer to pay $345,178 in fines and remedy its violations of the California Consumer Privacy Act (CCPA). Specifically, and as set out in the Stipulated Final Order, the retailer:

- Had a misconfigured opt-out mechanism for a period of 40 days, which prevented consumers from effectively opting out of the sale or sharing of their personal information. Businesses are reminded to monitor and validate that their third-party privacy management tools are working as expected;
- Required consumers to provide more information than necessary to process their opt-out requests, including government-issued identification, which is not permitted under the law. Businesses are reminded that data minimization is a core expectation and should only request information necessary to complete a request, such as the information required to identify the consumer within their own systems.

In addition to the hefty fine, the retailer agreed to:

- Identity and develop procedures to identify what personal data it is sharing and selling, and modify its current mechanism for enabling consumers to submit requests to opt out of sale/sharing, and implement procedures to ensure that its methods for submitting opt-out requests are compliant under the law;
- Not require consumers to provide more information than necessary to process a rights request;
- Develop, implement, and maintain training to ensure that all personnel handling personal information are informed of the business's requirements under the CCPA; and
- Maintain a contract management and tracking process to ensure that contractual terms required by the CCPA are in place.

23andMe

The genetic testing company, 23andMe, is back to selling its assets in bankruptcy. This deal raises significant concerns from both a privacy and cybersecurity perspective, as the acquisition transfers data from one of the largest private genetic databases.

- The acquisition raises questions about how sensitive genetic and personal data may be used by Regeneron, a company acquiring assets out of bankruptcy.
- **Why is this bankruptcy issue important?** It reiterates a long-held precedent that when a company acquires another company's data assets, it is obligated to uphold the acquired company's privacy policies. If the acquiring company materially changes how it plans to use and share the consumer's data, then it needs to obtain consumer consent.

Intern Elyssa Eisenberg contributed to this post. She is not currently admitted to practice law.

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Breach

Data Privacy, AI & Cybersecurity

Government

Website Data Privacy

Subscribe to receive timely legal insights directly in your inbox.