Technology Law Updates

California legislature clarifies privacy obligations for AI models

Andrew Folks, September 2, 2024

The intersection of privacy and AI just took on a new dimension in the Golden State. On August 30, 2024, the California Senate passed AB 1008, amending the California Consumer Privacy Ac to include personal information in various formats, including in artificial intelligence models. Onc signed, the bill will impose additional consumer privacy law obligations regarding models trained on such data. It now goes to the governor, who has until September 30 to veto.

What does AB 1008 say?

The bill revises the CCPA’s definition of “personal information” to include, among other things, “abstract digital formats, including … artificial intelligence systems that are capable of outputting personal information.” It also clarifies that “publicly available information" – exempted from “personal information” – does not mean “biometric information collected by a business without the consumer's knowledge.”

The bill’s author, Representative Rebecca Bauer-Kahan, likened text-based generative AI systems to data compression in justifying her bill. She asserted that, without her amendments, “ business could conceivably use a language model to compress personal information and transfe it to a buyer,” bypassing the CCPA's rules for the sale and share of personal information.

AB 1008 passed in tandem with SB 1223, which added neural data as a category of sensitive personal information.

Does an LLM trained on personal information contain personal information?

If so, consumers will have privacy rights related to the model itself. They could request deletion or correction, and businesses must remove or amend any data, such as tokens, model weights, or other data points, derived from personal information about that consumer that could lead to a output of personal information.

Regulators have been divided on this question since researchers found that personal informatio in training data could be extracted from LLMs. The California Privacy Protection Agency voted to support the bill following a staff position paper. The Hamburg Data Protection Authority disagreed, declaring: “Given that no personal data is stored in LLMs, data subject rights as defined in the GDPR cannot relate to the model itself.” With AB 1008, the California legislature has made its position clear.

Takeaways

Until now, privacy law compliance for AI models focused on collection, disclosure, and opt outs regarding personal information in model training. Following AB 1008, business obligations regarding California privacy law will continue beyond a model’s training phase. Businesses will need to respond to consumer requests with respect to access, deletion, correction, and sale/sharing of personal information.

The bill may create challenges given developers’ current inability to retroactively remove or alter information in their AI models. For instance, a business cannot simply remove specific information from a trained model, so a consumer deletion request may require the business to retrain or fine-tune its model without that consumer’s information.

One cost-reducing solution could involve temporarily suppressing a consumer’s personal information in a model’s outputs, and retraining or fine-tuning it without designated personal data every 90 days — the maximum allowable timeline to effectuate a request, with explanation to the consumer. This option will likely only be technically feasible for smaller, locally-hosted LLMs due to the associated retraining costs.

Looking forward, businesses should consider training models without personal information entirely, or only on publicly available information or properly de-identified or aggregated information. These information types are not considered personal information and would not be subject to the CCPA.

AI