California's New Account Deletion Law Is a Compliance Iceberg for Social Media Platforms

Alexis Keenan *Published November 19, 2025*

Major social media platforms will soon be subject to a new law in California that entitles users to a conspicuous “delete account” button that can erase their personal data from the clutches of Big Tech.

The law’s deceptively simple text is expected to trigger a nationwide and even global response from platforms, and could expose those that fail to comply to a range of risks. AB 656, which Gov. Gavin Newsom signed into law last month, is enforceable starting Jan. 1, 2026.

In essence, the law amends California’s Civil Code so that platform users are more empowered to wipe their valuable personal data from their social media accounts, without platforms slowing down or hindering that process.

The rule applies to large social media platforms that generate more than $100 million in annual gross revenue, such as Facebook, Instagram, LinkedIn, Snapchat, TikTok, YouTube, and X. Violators could be subject to administrative enforcement action, fines of up to $7,988, and potential liability in litigation.

Building on the Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), it provides that the platforms must treat a user’s "request to delete" as a request to remove their account and associated data. The law’s text says the platforms must offer a “clear and conspicuous” delete button and steer clear of obstructing delete requests, including through the use of “dark patterns” that complicate the process.

Platforms have 45 days to process and fulfill data deletion requests.

The law sponsored by Assemblymember Pilar Schiavo follows years of complaints from social media users who said their requests to remove their accounts and data went unfulfilled.

Global impact and compliance hurdles

Maryam Meseha, a data privacy and cybersecurity attorney and founding partner at Pierson Ferdinand LLP, said AB 656 could create compliance implications beyond the Golden State, as platforms are likely to offer the easy-delete process to users outside of California.

“Even though AB 656 is a California law, most large platforms will implement these standards nationally, and even globally, because maintaining separate systems for different jurisdictions creates unnecessary operational risk and user friction,” Meseha said.

Jeffrey R. Glassman, a data privacy and intellectual property lawyer and partner with Ervin Cohen & Jessup LLP, agreed.

“I think there's no way for social media companies across the globe to avoid the law’s basic requirements,” he said.

“While the law is oriented towards protecting citizens of California, it applies to any company who is attracting business from California consumers,” he explained, adding that a single person could trigger obligations under the law.

Glassman and other data privacy lawyers cautioned that an overly simple approach to AB 656 compliance could backfire. They warned that the

law's text appears straightforward, but in reality is jam-packed with complex backend requirements that could demand work from teams of computer programmers.

"It's a massive undertaking," Glassman said.

The "easy part", Glassman said, is the design adjustments that platforms need to make to incorporate a digital delete button that users can easily see when they're logged into their accounts.

But the heavier compliance burden, he said, is mapping data flows programmed on the back end of a platform, where personal information is stored and shared. "That's especially true for companies that are making use of server farms and databases located outside of this country," Glassman said.

Another problem with a lax approach to compliance is that it could overlook user data that platforms share with third parties.

"I think [platforms] are going to have to be especially hard working and sensitive to the fact that they need to know where all the data resides," Glassman said.

For those reasons, Danie Strachan, senior privacy counsel for data privacy compliance advisor VeraSafe, said legal advisors need to work closely with their clients' technical teams to map data flows. Legal counsel should also ensure that companies train employees that execute AB 656's technical requirements to ensure they eliminate all user information that the law requires.

Strachan warned that AB 656's design and data mapping obligations are absolute, so platforms must be sure that when their users click "delete," they can deliver on that promise across all systems, databases, and backups.

"Modern social media architectures are incredibly complex, with user data distributed across production systems, analytics platforms, content delivery networks, and disaster recovery infrastructure," he said. "Organizations must develop comprehensive data mapping and deletion procedures that account for every instance of user information within the scope of a deletion request under AB 656, while maintaining system integrity and meeting other legal obligations."

On top of that, Strachan said that the law's prohibition of dark patterns is equally challenging because it requires platforms to resist their natural inclination to retain users: "they must design interfaces that are genuinely user-friendly rather than subtly manipulative."

"What many organizations haven't fully grasped is that this law has caused a shift in the power dynamic between platforms and users, and it's not just about checkbox compliance; it's about recognizing users' right to control their own digital presence," Strachan said.

"Legal advisors must help their clients understand that this isn't just about adding a button," he continued. "It's about fundamentally rethinking user experience design to eliminate friction in the deletion process."

The AI effect

As with most technology endeavors today, data privacy lawyers expect artificial intelligence to influence AB 656 compliance.

“As AI becomes more deeply embedded into consumer and enterprise platforms, the volume and sensitivity of personal data in these systems process will grow exponentially,” Meseha said. “This raises complex questions around data retention, model retraining, and whether ‘deletion’ can truly occur once data is used to inform algorithmic outputs.”

She predicts that deletion requirements will extend to AI products and services that have access to a platform’s users’ personal data, especially those that rely on vast datasets for model training and personalization.

Platforms therefore need to ensure that deletion requests not only remove visible user accounts but also extend to underlying data used for training AI models, analytics, and recommendation engines.

To stay in line with those rules, Meseha explained, companies should adopt a “privacy-by-design” framework by building deletion capabilities into their product’s full data lifecycle, from collection and storage to downstream processing.

Operationally, she said, handling linked or derivative data in AI systems is one of AB 656’s biggest compliance challenges, in addition to synchronizing deletion across multiple databases and vendors. Another, she said, is maintaining auditability to prove that compliance.

Exceptions to the rule

Not all data is required to be deleted under AB 656, even if an account holder requests it.

Lydia Liberio, a mediator and arbitrator at the nonprofit Mediation Center for Los Angeles and a civil litigator with expertise in consumer rights, said AB 656 is a "significant" development for consumers, data brokers, and technology compliance departments, but is still subject to exceptions under California's privacy laws.

The laws permit platforms to retain data that they need to maintain current business-consumer relationships, she said. They also allow platforms to retain certain data that they obtained directly from consumers, as well as data subject to litigation holds or government investigations. Another exception is data from consumers whose deletion requests cannot be verified as authentic.

However, Liberio noted that it's not clear how AB 656's focus on personal data held by social media platforms will apply to data caught up in mergers and acquisitions between data brokers. Nor is it clear what happens when a data broker holding such information files for bankruptcy -- and its assets, including consumer data, are sold off by out-of-state receivers.

"Platforms should clarify with legal counsel which of their activities may trigger data broker issues," Liberio said.

Another newly amended California law, SB 361, requires data brokers carry out consumer data deletion requests within 45 days. The tougher standards, which strengthen the Data Erasure Law for Enhanced Transparency and Enforcement Act ("DELETE" Act"), says that data brokers

must process a user's delete request in a transparent, trackable way, using a required Delete Request and Opt-Out Platform ("DROP"). The platform is scheduled to go live January 1, 2026.

The law, first enacted in 2023, requires brokers to register directly with the CPPA.

Penalties and reputational risks

A platform's failure to adhere to AB 656 can lead to administrative enforcement action, fines, and potentially private lawsuits from aggrieved account holders.

The law specifies enforcement to be carried out by the CCPA's independent regulator, the California Privacy Protection Agency (CPPA), created by the California Consumer Privacy Act of 2018. Under Civil Code section 1798.155, the agency can investigate compliance issues, hold hearings, and assess fines for non-compliance.

Allowable penalties follow the CCPA's already established penalties for violations of the DELETE Act. Fines for violations increased in January from up to $2,500 to up to $2,663, per violation. Steeper penalties can be assessed for intentional violations and violations involving personal information of an account holder that a platform knew to be under age 16. Those jumped from up to $7,500, per violation, to $7,988.

Strachan, VeraSafe's lawyer, said that the potential penalties may appear insubstantial for social media platforms that generate billions of dollars in revenue each year, but the reputational and operational risks of

enforcement action are considerable.

“The real deterrent isn't necessarily the per-violation amount,” he said. “It's the potential for systematic non-compliance to result in massive aggregate exposure.”

“For these platforms, regulatory scrutiny and the associated compliance costs, legal fees, and business disruption can be far more damaging than the fines themselves,” he continued.

There’s no private right of action for aggrieved account holders under AB 656. However, Meseha said it may give more leverage to plaintiffs who want to sue over wrongly retained data.

“While AB 656 doesn’t grant users a direct right to sue, it strengthens their position in a few indirect ways,” Meseha said. “For one, clear deletion requirements make it easier to demonstrate harm if a company fails to comply — for example, in the event of a data breach involving information that should have been deleted.”

Additionally, she said, noncompliance could be cited in consumer protection or unfair business practice claims, creating a litigation hook. “In short, users may not have new rights on paper, but they’ll have stronger evidence of negligence or unfair conduct in disputes with platforms,” Meseha said.

Glassman agreed, and said he would expect plaintiffs’ lawyers to pursue alleged violations of AB 656 under California’s broad statute prohibiting unfair business practices. In large enough numbers, he said, even single-

digit thousand-dollar damages could add up to multi-millions.

Consumer frustration and national implications

It's too soon to know whether AB 656 will set a national precedent for account deletion requests.

Over time, Meseha said, the statute could drive a de facto national standard for user deletion rights, much as the CCPA influenced broader corporate privacy policies before other states followed suit.

David Hoppe, a technology and media attorney and the founder of Gamma Law, left room for skepticism. Despite the common assumption that AB 656 will have a ripple effect in the absence of a federal data privacy law, he said broad adoption by other states may never happen.

"I wonder if we're getting to a point where some of the big players may say: 'We're tired of having one state dictate the entirety of our national compliance," he said.

Hoppe said that nonetheless, the platforms are going to have to face the music in California.

"I have no sympathy for them," he said, citing his own struggle to circumvent dark patterns that impeded his request to delete a social media account. "They collected the information, and they know where they put it and who they gave it to, and they need to give it back."

Tony Anscombe, "chief security evangelist" for the global cybersecurity

provider ESET, said California consumers first gained the right to know, access, and delete their data more than five years ago, under the CCPA. But in practice the law didn't fully empower platform users to erase their personal information, because many online companies retained the data by using dark patterns and placing other obstacles in the path of deleting an account.

Anscombe said that he too recently experienced roadblocks to erasing his social platform account and data. In his case, he said, the platform's instructions for deleting his account misstated the location of the delete option.

"Removing friction and allowing consumers to exercise their rights to delete data that a company holds on them should never have been an issue," he said. "The law is just stopping companies from making it a difficult process."

The unmet requests were by design, according to research published in 2022 by the University of Chicago and the U.S. Federal Trade Commission (FTC). In the study, which was cited in Schiavo's legislation, researchers found that across the social media landscape, "delete" options tended to obscure the meaning of the word.

Instead of permanently deleting the data, the platforms frequently treated the requests as requests to "deactivate" or "hide" a user's account.

The study also found that true account deletion often required users to take multiple unnecessary steps, provide layers of verification, and access their accounts on particular devices or in particular device modes. Even after completing multiple steps, the researchers said, certain "deleted"

accounts reappeared.

Another report published by the FTC in September 2024 found that major social media platforms and streaming companies were collecting "troves" of personal data from their users, as well as non-users, and that the collected data could be retained by the companies indefinitely.

The FTC's findings were drawn from orders for information that it sent to nine of the largest social media platforms and video streaming companies, including Amazon's Twitch, Meta's Facebook, Alphabet's YouTube, X, Snap, ByteDance's TikTok, Discord, Reddit, and WhatsApp.

Both studies concluded that the platforms were incentivized to prevent users from leaving so that they could continue monetizing user information, mostly through targeted advertising.

CEB did not receive responses from the platforms mentioned in this article inquiring how their users' platform experience would change after AB 656 goes into effect in January.