SENATE THIRD READING
SB 361 (Becker)
As Amended June 26, 2025
Majority vote

SUMMARY

This bill, sponsored by Oakland Privacy, expands the types of information that data brokers must disclose that they collect which will then be displayed on the data broker registry. Specifically, it requires data brokers to indicate whether they are collecting account logins and account numbers, driver's license numbers and other types of identification numbers, citizenship data, union membership data, sexual orientation data, gender identity and expression information, and biometric information. Furthermore, this bill would increase transparency by requiring data brokers to disclose when registering whether they have sold or shared consumers' information with a foreign actor, the federal government, other state governments, a law enforcement agency, or a developer of an AI system or model in the past year.

Major Provisions

1) Requires data brokers registering with the California Privacy Protection Agency (Privacy Agency) to indicate whether they collect the following information on consumers:

    a) Account login or account number in combination with any required security code, access code, or password that would permit access to a consumer's account with a third party;

    b) Drivers' license number, California identification card number, tax identification number, social security number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

    c) Citizenship data, including immigration status;

    d) Union membership status;

    e) Sexual orientation status;

    f) Gender identity and gender expression data; or

    g) Biometric data.

    h) Whether the data broker has shared or sold consumers' data to a foreign actor in the past year.

    i) (Whether the data broker has shared or sold consumers' data to the federal government in the past year.

    j) Whether the data broker has shared or sold consumers' data to other state governments in the past year.

    k) Whether the data broker has shared or sold consumers' data to law enforcement in the past year.

l) Whether the data broker has shared or sold consumers' data to a developer of an AI system or model in the past year.

COMMENTS

Why protecting personal information is important. Some may consider sharing their private information, including websites they visit, purchases, employment history, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, failing to actively protect our private information can have real world consequences. As an example, dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal information with advertisers, including location, sexual orientation and mental health details.[1] This was not the first time Grindr had failed to protect their users' private information. Several years earlier, it was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[2]

More recently, a hack of the location data analytics company Gravy Analytics revealed that precise geolocation data was being collected from thousands of apps, including Candy Crush, Tinder, and even many VPN apps, which ironically are intended to enhance user privacy.[3] The hack exposed that app developers themselves were often unaware of this tracking, as the data was gathered through advertisements embedded in the apps. Gravy Analytics aggregated this geolocation data and sold it to advertisers and government entities, including the U.S. federal government. The fact that this data was collected without the knowledge of either users or developers underscores serious concerns about the reach and practices of data brokers.

Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), consumers are granted a range of privacy protections, including the right to transparency, notice, correction, deletion, and the ability to opt out of data collection. However, enforcing these rights has proven challenging due to the opaque practices of data brokers like Gravy Analytics. These entities rarely interact directly with consumers. Instead, they collect data by partnering with businesses, purchasing data from other brokers, or scraping the internet to compile detailed consumer profiles. This creates a system in which consumers are unaware that their data is being collected, let alone what data is being held or where it came from. In December, the Federal Trade Commission (FTC) took enforcement action against Gravy Analytics, alleging the company had sold non-anonymized location data in violation of consumer protection standards, resulting in a prohibition in the selling and sharing of sensitive location data.[4]

---

[1] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[2] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
[3] Joseph Cox, "Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location", *Wired* (Jan. 9, 2025), https://www.wired.com/story/gravy-location-data-app-leak-rtb/.
[4] Federal Trade Commission, "FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data" (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-gravy-analytics-venntel-selling-sensitive-location-data.

California has made strides to address this lack of transparency. AB 1202 (Chau, Chapter 753, Statutes of 2019) established the state's data broker registry, requiring brokers to register and disclose certain practices. Brokers must now report if they collect sensitive categories such as precise geolocation or reproductive health data. Yet, for most consumers, it remains nearly impossible to know what personal information is being collected or how it may be used.

This lack of visibility is especially concerning when data broker information can be used punitively. For example, recent increases in U.S. Immigration and Customs Enforcement (ICE) activity have raised alarms about the use of brokered data to bypass sanctuary laws, an issue already documented in Colorado.[5] Employers could potentially access brokered data to discriminate against job applicants with a history of union involvement. Similarly, data revealing gender identity or sexual orientation could be exploited to harass, intimidate, or dox individuals.

To help address these risks, SB 362 (Becker, Chapter 709, Statutes of 2023) strengthened consumers' rights by establishing a centralized data deletion mechanism. Beginning in 2026, consumers will be able to submit a single deletion request form, requiring all registered brokers to delete their personal information, and to continue deleting any new data collected every 45 days thereafter. The law also requires brokers to disclose whether they are regulated under specific state and federal laws and to include this information on the California Privacy Protection Agency's website. Beginning in 2028, data brokers will also be subject to third-party audits to verify compliance with SB 362.

Despite these advances, consumers still deserve a clear understanding of what types of sensitive information are being collected and traded by data brokers, and how that information could potentially be used against them.

According to the Author

> Californians have a right to know who is collecting their most sensitive personal information. SB 361 increases transparency in the data broker industry, helping people protect their privacy.
>
> There are serious concerns that data brokers are selling sensitive information in ways that could lead to surveillance and targeting of vulnerable communities, including immigrants, and LGBTQ+ individuals. The risks of mass deportation, discrimination, and other harmful outcomes are real, and we must act to protect people's privacy.
>
> Building on the California Delete Act, which was passed in 2023, SB 361 requires data brokers to disclose whether they collect sensitive information like government IDs, union membership, and sexual orientation. The California Privacy Protection Agency (CPPA) will publish this information, empowering Californians to make informed decisions about their privacy and will soon have the ability with the click of a single link to delete their personal data and prevent it from being sold.

---

[5] Johana Bhuiyan, "US immigration agency explores data loophole to obtain information on deportation targets", *The Guardian* (Apr. 20, 2022), https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets.

California has long been a leader in privacy protections, and SB 361 ensures that individuals—not data brokers—remain in control of their personal information.

Arguments in Support
Oakland Privacy, the sponsor of the bill, write in support:

The premise of SB 361 is that Californians have a right to know which companies have obtained and are prepared to sell their highly sensitive information and to be able to distinguish those particular data brokers from those who are distributing less sensitive information. We absolutely agree that both consumers and regulators should have access to this information, and most importantly, that gaining that access should not be a burdensome process for consumers.

The bill requires data brokers to disclose when they register whether or not they collect certain kinds of specific information that can be considered sensitive or high-risk for the individuals in their databases including:

1) log-in data like user names, passwords, and account numbers

2) governmental identifier numbers like social security numbers, drivers license numbers or military IDs

3) citizenship data and immigration status

4) information about sexual orientation and identity

5) information about union membership and activism

6) biometric data including faceprints, iris prints, palm prints, voiceprints, gait indicators and neural data.

Sensitive or high risk data is information that consumers need to protect for specific reasons, which can include identity theft and identity verification, as well as potentially negative ramifications if information sold by third parties gets into the wrong hands including blackmail, threats to employment and deportation.

The initial iteration of the registry asks the data broker registrants three questions about what they collect: whether they collect the information of minors, whether they collect geolocation data, and whether they collect data about reproductive health care. SB 361 would ask the same questions about six more categories of sensitive information which are listed above.

While the DROP mechanism is intended to allow Californians to opt out from all registered data broker data sales and profiling, the additional information that would be provided by the bill would be helpful to consumers in several ways:

1) To focus on the particular companies that collect personal information they are particularly worried about safeguarding and ensure that the DROP process worked for them if they chose to use it.

2) To motivate consumers to use the DROP service if they need it, by helping them to understand in more specificity what kinds of personal information is being collected and is potentially being sold.

3) To assist regulators and legislators to have a better understanding of the specifics of data broker marketplaces and to identify and address new risks as they develop as technology continues to innovate, creating new methodologies for the use and misuse of sensitive personal information.

We don't believe that the additional information that would be added to the data broker registration process is particularly burdensome to the companies. They know what they collect. It is only the consumer who doesn't know this information.

Arguments in Opposition
None on file.

FISCAL COMMENTS

According to the Assembly Appropriation Committee:

CPPA reports absorbable near-term costs to update its data broker registration website and for enforcement. Costs may be offset to some extent by registration fees CPPA is authorized to charge. The agency anticipates it may need additional resources for enforcement in the future, depending on data brokers' compliance with the bill's requirements.

VOTES

SENATE FLOOR: 37-0-3
YES: Allen, Alvarado-Gil, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Choi, Cortese, Dahle, Durazo, Gonzalez, Grayson, Grove, Hurtado, Jones, Laird, Limón, McGuire, McNerney, Menjivar, Niello, Ochoa Bogh, Padilla, Pérez, Richardson, Seyarto, Smallwood-Cuevas, Stern, Strickland, Umberg, Valladares, Wahab, Weber Pierson, Wiener
ABS, ABST OR NV: Archuleta, Reyes, Rubio

ASM PRIVACY AND CONSUMER PROTECTION: 15-0-0
YES: Dixon, Bennett, Bryan, DeMaio, Irwin, Lowenthal, Hoover, McKinnor, Ortega, Patterson, Pellerin, Petrie-Norris, Ward, Wicks, Wilson

ASM APPROPRIATIONS: 15-0-0
YES: Wicks, Sanchez, Arambula, Calderon, Caloza, Dixon, Elhawary, Fong, Mark González, Hart, Pacheco, Pellerin, Solache, Ta, Tangipa

UPDATED

VERSION: June 26, 2025

CONSULTANT: John Bennett / P. & C.P. / (916) 319-2200 FN: 0001112