April 10, 2026

Chair Rebecca Bauer-Kahan
Vice Chair Alexandra Macdeo
Committee on Privacy and Consumer Protection
California Assembly
Legislative Office Building
1020 N Street, Room 162
Sacramento, CA 95814

RE: AB 1542 (Ward) – SUPPORT

Dear Chair Bauer-Kahan and Vice Chair Macedo,

Consumer Reports is proud to co-sponsor AB 1542, legislation that would amend the California Consumer Privacy Act (CCPA) to ban the sale of consumers' sensitive personal information. While there are plenty of valid reasons for businesses to *collect* and *use* our sensitive personal information to provide products and services as requested, they should not be *selling* this information behind our backs. This bill will put an end to that practice, providing default protections that preserve the privacy, autonomy, and physical safety of Californians.

For obvious reasons, consumers have a strong interest in keeping their sensitive personal information as private as possible, even if they must share it with companies to receive a product or service. Recognizing this, CCPA provides additional protections for sensitive personal data, which includes personal information that falls into one of the following categories: 1) government identification numbers, 2) financial account information or credentials, 3) precise geolocation information, 4) racial or ethnic origin, 5) citizenship, immigration status, 6) philosophical beliefs, 7) union membership, 8) contents of private messages, 9) genetic or neural information, and 10) information about one's health or sex life.

Unfortunately, California's sensitive data protections lag behind those of other states with comprehensive privacy laws, which generally prohibit the processing of sensitive personal information absent consent. In order to protect themselves, California consumers must affirmatively opt out or invoke their right to limit sensitive information — a right that few consumers likely even know exist, let alone how to exercise. As a result, consumers' sensitive information is regularly sold to hundreds of third-parties without their awareness.

The widespread abuse of consumers' sensitive data leads to a variety of harms, including, but not limited to:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use commercially available sensitive data, such as **consumers' precise geolocation**, to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use location information to increase the specificity of their phishing or social engineering scams, such as by including location-specific details like mentioning a nearby business or the individual's recent activity.[1] Location data is also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[2] Location data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day,[3] reportedly suffered a massive data breach that may have leaked the location information of millions of individuals.[4] This type of information makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[5]

- *Unexpected sharing of non-CMIA-covered health information.* Many companies that collect **information concerning consumers' health or sex lives** are failing to safeguard it. For example, Consumer Reports' recent investigation of several major exercise equipment companies found that it was common for companies to give themselves permission to sell health-related information to marketing and social media companies.[6] And an earlier Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.[7]

  Additionally, the Federal Trade Commission has recently enforced against several companies that improperly shared personal health information with third-parties or broke

---

[1] Phishing Box, Tracking Data: Identifying the Anonymized, https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized
[2] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs
[3] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf
[4] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/
[5] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf
[6] Catherine Roberts, Your Exercise Bike Knows a Lot About You—and It Doesn't Keep Every Secret, Consumer Reports, (January 14, 2025), https://www.consumerreports.org/health/health-privacy/exercise-machine-privacy-a3907557984/
[7] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

their privacy promises to consumers, including fertility tracker apps Flo[8] and Premom[9], online counseling service BetterHelp[10], and online prescription company GoodRx.[11] A blanket ban on the sale of sensitive data would've gone a long way toward avoiding these harms before they were detected by regulators.

- *Predatory use of consumer data.* Marketers and ad-tech companies regularly sell information about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this information collection and sale. In some instances, this can result in financially disastrous consequences for consumers. Some marketers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products.[12] Other marketers sell lists of individuals based on their **religious beliefs** or **sexual orientation,** sourced from the use of certain prayer or dating apps.[13]

  Meanwhile, the pervasive sale of consumer's sensitive information, including information revealing consumers' **immigration or citizenship status**, in the real-time ad bidding context creates the opportunity for unexpected secondary uses by federal law enforcement. The Department of Homeland Security and Immigration and Customs Enforcement recently released a Request for Information on "how the industry's commercial Big Data and Ad Tech providers can directly support investigations activities."[14]

---

[8] Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

[9] Federal Trade Commission, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order, (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

[10] Federal Trade Commission, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, (March 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

[11] Federal Trade Commission, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, (February 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

[12] Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[13] Jon Keegan and Alfred Ng, the Markup, Gay/Bi Dating App, Muslim Prayer Apps Sold Data on People's Location to a Controversial Data Broker, (January 27, 2022) https://themarkup.org/privacy/2022/01/27/gay-bi-dating-app-muslim-prayer-apps-sold-data-on-peoples-location-to-a-controversial-data-broker

[14] Department of Homeland Security, Request for Information, RFI Big Data & Ad Tech, (January 23, 2026), https://sam.gov/workspace/contract/opp/411452e8b3614944b9c50cc3aa24fb42/view

- *Enhanced risks of data breaches and identity theft.* Data brokers collect trillions of data points on Americans, including sensitive data like **social security numbers, state identifiers, and other financial account information** that can be used for identity theft, so they are unsurprisingly a top target for hackers and cyber criminals. Just last month, Congress' Joint Economic Committee released a report linking just four recent individual data broker data breaches to over $20 billion in losses to consumers.[15] The true overall cost to consumers is likely much higher.

AB 1542 will address the above described issues by simply updating CCPA to ensure that businesses only collect and use consumers' sensitive data to provide the products and services they expect — and will prevent the sale of such information to data brokers and big tech advertising companies.

Industry interests will likely insist that sensitive data should continue to be regulated through a consent-based framework. But we already know that doesn't work. While many other states currently use a stronger opt-in (as opposed to CCPA's opt-out) standard for sensitive data, this has not stemmed the tide of data abuses. In those states, many businesses simply *require* you to consent to the sale of your sensitive data as a condition of using the service, or infer blanket consent for any secondary uses when a consumer provides data as part of using a service. This type of structure fails to meaningfully protect consumers. And ultimately, forcing consumers to make constant consent choices is not the solution to this problem. Instead of playing the cat-and-mouse consent game, privacy laws should simply prohibit inherently harmful uses of consumer data.

Indeed, this legislation would help California join the movement of states heading in that direction. For example, in 2024 Maryland banned the sale of all sensitive information as part of its comprehensive law. Last year, Oregon also banned the sale of certain subsets of sensitive information. And this year, several states are considering similar bans, including in Maine, Massachusetts, and Vermont. Californians deserve the same level of protection.

For these reasons, Consumer Reports is proud to sponsor AB 1542, and we urge the committee to approve it.

Sincerely,

Matt Schwartz
Senior Policy Analyst
Consumer Reports

---

[15] United States Joint Economic Committee, Minority Report, Ranking Member Senator Maggie Hassan, Opt-Out Obstacles: Concerning Practices by Registered Data Brokers and the Multi-Billion-Dollar Cost of Breaches, (February 2026), https://www.jec.senate.gov/public/_cache/files/7f821956-d826-4241-8196-be987cc1f06c/2026-02-27-jec-data-brokers-report-final.pdf