Vermont Delete Act FAQ

What is the Vermont Delete Act?

The Vermont Delete Act builds upon the Vermont Data Broker Registry to address significant cybersecurity and privacy harms associated with data brokers — shadowy companies with whom we don't have a direct relationship that buy and sell our personal data to anyone with a credit card and do so without our knowledge and consent.

The bill requires the following:

- *Disclosure of Sensitive Categories of Data Collected*: data brokers must register with the Secretary of State and disclose if they collect and sell sensitive personal data such as precise geolocation, reproductive healthcare data, immigration status, sexual orientation, and Social Security Numbers.
- *Provide Notice of Security Breaches and Verify Who They Sell Our Data To*: data brokers must protect our personal data and provide notices of data breaches to the Attorney General. Furthermore, data brokers must take reasonable procedures to ensure that personal data is sold for legitimate and legal purposes.
- *Accessible Deletion Mechanism*: the Secretary of State must set up an easy-to-use "one-stop" website that allows individuals to make a single and one-time deletion request for all data brokers. This avoids the "whack-a-mole" game that consumers now experience of having to spend hundreds of hours manually contacting hundreds of data broker sites and making one-by-one requests — and then seeing the data brokers simply re-populating their databases with consumers' data.

What is a one-sentence description of the Vermont Delete Act?

The bill would require data brokers to disclose categories of sensitive data they collect and sell, provide a notice of security breaches, certify that the personal information they disclose will be used for a legitimate purpose, and empower consumers to easily get their data deleted from data brokers via a website maintained by the Secretary of State.

So, what are data brokers?

Data brokers are defined as businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship. Unlike Big Tech firms like Meta and Google, which primarily collect our online activity, data brokers collect information about us from online and offline sources, thus surveilling us just as significantly. Data brokers' data sources include property records, purchase history, social media profiles, and online web and mobile app activity tracking — including tracking our precise geolocation and all the websites we visit. Data brokers then aggregate our data into massive digital dossiers and then either sell or share our data with third parties. Data brokers have been in the headlines lately

because of massive data breaches and instances of selling highly personal data to fraudsters or foreign entities.

What are some of the recent issues with data brokers?

Data brokers represent a growing threat to privacy, civil liberties, and national security.[1] Data brokers have been found to enable aggressive targeting of vulnerable populations such as “economically anxious elders,” “heavy purchasers of pregnancy tests,” and “frequently depressed.”[2] Recently, a data broker was found selling lists of people undergoing chemotherapy to cremation companies.[3] Texas Attorney General Paxton sued Allstate and its data broker subsidiary over illegally tracking drivers and causing consumers’ car insurance to go up.[4] And the Protecting Americans’ Data from Foreign Adversaries Act (“PADFAA”) was recently passed on a bipartisan basis due to the issue of data brokers selling Americans’ sensitive personal information — including data of military personnel — to foreign bad actors.[5]

Data brokers’ business model can also facilitate identity theft. As cybersecurity journalist Brian Krebs notes, data from data brokers is beneficial for hackers trying to determine the maiden name of someone's mother or successfully answer a range of other knowledge-based authentication questions.[6] Thus, the larger the data brokers’ digital profile of consumers, the easier it is for cybercriminals to use that data to target consumers, devise pretexts, and plan social engineering attacks. Not surprisingly, it turns out that 92% of cyber-attacks are specifically crafted from users’ OSINT (i.e., open-source intelligence such as public information about people), according to Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA).[7]

---

[1] Office of the Director of National Intelligence, Declassified Report on Commercially Available Information (CAI) January 2022, at 3, 8, https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf, stating, "There is today a large and growing amount of [Commercially available information] that is available to the general public, including foreign governments (and their intelligence services) and private-sector entities, as well as the [Intelligence Community]. . . It also raises significant issues related to privacy and civil liberties."

[2] https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[3] https://www.adexchanger.com/data-driven-thinking/what-do-we-say-to-emily-the-human-cost-of-advertising-data-abuse/.

[4] https://autos.yahoo.com/allstate-sued-texas-allegedly-collecting-193000584.html.

[5] CFPB Director Rohit Chopra noted that data brokers’ sale of Americans’ personal information "raises significant privacy, counterintelligence, blackmail risks, and other national security risks—especially for those in the military or national security community.” https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-national-security/.

[6] https://krebsonsecurity.com/2024/03/a-close-up-look-at-the-consumer-data-broker-radaris/.

[7] Jen Easterly, Presentation to Engineering Capital. October 30, 2019.

Identity theft and cybercrime facilitated via data brokers specifically target the elderly. For example, the data broker InfoUSA allegedly sold a list of 19,000 elderly sweepstakes players to a group of experienced scam artists. The scam artists then stole over $100 million by calling the victims and impersonating government officials who needed the victims' bank account information. Another example is the FTC fining the data broker firm Epsilon $150 million for allegedly helping to facilitate elder fraud scams.[8]

Finally, lax cybersecurity practices by data brokers represent a real and significant threat to citizens. The data broker National Public Data was hacked in 2023, resulting in over a hundred million Americans now having their Social Security Numbers (SSNs) in hackers' hands.[9] And the data broker Gravy Analytics made headlines in January 2025 when hackers stole terabytes of consumers' precise geolocation data, thereby showing peoples' precise movements.[10]

What is the Vermont Delete Act modeled after?

The accessible deletion mechanism is modeled after the federal bipartisan proposal known as the DELETE Act that was introduced by Senator Cassidy (Republican) of Louisiana and Senator Ossoff (Democrat) of Georgia.[11] A California version of the DELETE Act was signed into law in 2023.[12] Furthermore, the bill was written to provide consistency with other state data broker laws (Oregon, California, and Texas).

Does the Vermont Delete Act build upon the Vermont Data Broker Registry?

Yes. This bill was carefully written to embrace and extend the Vermont Data Broker Registry to address the cybersecurity and privacy harms associated with shadowy data brokers that collect and sell our most personal data. This bill addresses real-world harms associated with data brokers, such as selling our personal data to foreign nations and the recent massive cybersecurity breaches involving data brokers that have given hackers our Social Security Numbers and the ability to track our precise movements.

Who pays for the website that hosts the data broker registration and accessible deletion mechanism?

Data brokers pay a fee to be determined by the Secretary of State for the registration component of the bill. The reasonable cost to establish and maintain the accessible

---

[8] Paul Boutin, "The Secretive World of Selling Data About You," *Newsweek*, May 30, 2016, https://www.newsweek.com/secretive-world-selling-data-about-you-464789. U.S. Department of Justice, "Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes," January 27, 2021, https://www.justice.gov/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes.

[9] https://databreach.com/breach/national-public-data-2024.

[10] https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/.

[11] https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-ossoff-trahan-edwards-reintroduce-bill-to-protect-americans-online-privacy-and-data/.

[12] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362.

deletion mechanism will be equally borne in an additional fee paid by each data broker — determined by the Secretary of State annually. The goal is for this bill to be funded by data broker fees, not taxpayers.

Is the accessible deletion mechanism needed, i.e., can't a consumer manually make deletion requests?

As noted by a recent law review article: "Attempting to scrub one's Internet presence is a Hydra-like problem: although some sites allow users to request removal of their data, these hundreds, if not thousands, of data broker sites continuously repopulate their offerings by re-pulling their sources."[13]

Even if Vermont had a data broker registry that identified what data brokers are out there, the onus is still up to the consumer to contact every data broker to request opt-out and deletion. Assuming it takes thirty minutes per broker and there are five hundred brokers registered[14], opting out from all of them would require 250 hours of work per consumer!

Compare this to the "one-stop" website envisioned by the Delete Act — a consumer would have to spend a minute or so to direct their data to be deleted.

Who enforces the Vermont Delete Act?

The Attorney General and Secretary of State have full enforcement powers. An analogous example of an enforcement action that could happen under this law is Texas AG Paxton suing Allstate and its data broker subsidiary Arity for not registering under Texas' data broker law. This was part of a larger action against Allstate for allegedly "unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones through secretly embedded software in mobile apps."[15]

Another analogous example is the California Privacy Protection Agency (CPPA) fining multiple data brokers for not registering with the State of California.[16]

---

[13] Molly Cinnamon, *You Have the Right to Be Deleted: First Amendment Challenges to Data Broker Deletion Laws,* at 4 (Dec. 13, 2024), https://ssrn.com/abstract=5009948.

[14] California has over 500 registrations, and Vermont's registry has over 700, so this is a likely number. See https://cppa.ca.gov/data_broker_registry/ and https://therecord.media/state-data-broker-registries-california-vermont.

[15] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[16] https://cppa.ca.gov/announcements/2025/20250129.html,