ISSUE BRIEF U.S. Policy

THE BOUNDARIES OF DATA BROKERAGE

AN OVERVIEW OF THE U.S. REGULATORY LANDSCAPE

JULY 2026

FUTURE OF PRIVACY FORUM

AUTHOR

Jordan Francis, *Senior Policy Counsel*

ACKNOWLEDGEMENTS

Special thanks to the participants in FPF's May 2026 roundtable on data brokerage—comprising representatives from civil society, industry, and academia—for their insights. The author would also like to thank FPF U.S. Policy interns Kelly Brandmeyer, Gavin Bock, and Camille Herring for their research assistance.

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

Table of Contents

Executive Summary **4**
Introduction **5**
State Data Broker Laws **6**
Covered Entities 8
Covered Information 11
Registration and Business Obligations 13
Accessible Deletion Mechanisms and Third-Party Audits 16
Federal Data Broker Regulation **19**
Protecting Americans' Data from Foreign Adversaries Act 19
Recent FTC Enforcement Under Section 5 22
Policy Considerations **23**
Scoping: Types of Data and Entities Subject to Regulations 23
Use Cases: Broad Regulation of "Data Brokerage" versus Targeted Prohibitions 25
Safeguards: The Role of Existing Legal and Technical Protections 26
Conclusion **28**

Executive Summary

Data brokers have been the subject of intense scrutiny in recent years, including through critical media coverage, public hearings, private lawsuits, regulatory enforcement actions, and new state and federal regulatory frameworks. Despite all this public attention, there is little consensus as to who is a "data broker," what risks and benefits are associated with data brokerage, and how the evolving privacy regulatory landscape affects this industry.

The data broker industry is diverse, and the risks posed to individuals vary depending on data use cases, sensitivity, and companies' practices. Data brokerage also enables services widely regarded as beneficial, such as combating fraud and other illegal activities as well as enabling access to financial services. It also supports personalized marketing, toward which consumers and other stakeholders have a range of views.

This issue brief provides an overview of the emerging regulatory landscape, focusing on recently enacted state and federal laws that specifically regulate the data broker industry. This analysis highlights differences in these laws' scope and obligations. Key takeaways:

- **Inconsistent Scope:** New U.S. data broker laws define a data broker as either a business that sells personal data that the business did not collect directly from the consumer or sells the data of a consumer with whom the business does not have a direct relationship. Both approaches attempt to exclude the sale of data that was collected in a first-party interaction but differ in their formulation.
- **Requirements Include Registration, Security, and Targeted Prohibitions:** Data brokers are typically required to register with the state annually. Some of these laws include additional obligations such as maintaining adequate security or targeted prohibitions such as bans on fraudulent acquisition of personal data.
- **Accessible Deletion Mechanisms Are Paradigm-Changing:** Exercising deletion or opt-out rights on a company-by-company basis can be difficult and time-consuming for consumers. California's new accessible deletion mechanism, soon to be replicated in Connecticut, changes this calculus for consumers by enabling deletion requests en masse. Nevertheless, these tools may pose a risk to consumers in-and-of themselves if not implemented securely.
- **Existing Consumer Protection Law Remains Relevant:** As states experiment with data broker registries and Congress focuses on limiting the flow of sensitive data to foreign adversaries and countries of concern, longstanding consumer protection laws like the FTC Act remain an avenue for enforcement actions against data brokers.

The issue brief concludes with ongoing policy considerations that may prove valuable for future legislative efforts as well as industry practices. For policymakers, key questions include the appropriate scope of new regulations (both in terms of the types of data and entities who should be regulated), whether new frameworks should broadly define "data brokerage" or focus on specific harmful use cases, and how existing legal and technical protections can be better enforced or inform future regulatory frameworks. For industry, they include the extent to which organizations should adopt voluntary practices for transparency and data stewardship in order to deepen customer and public trust.

Introduction

Between high profile Congressional hearings,[1] headline-grabbing exposés by investigative journalists,[2] and detailed reports from academics and civil society organizations,[3] "data brokers" have been the subject of intense public scrutiny in recent years. As is often the case, that public scrutiny has translated into legal scrutiny. Data brokers are increasingly facing private lawsuits, enforcement actions by attorneys general and agencies, and new regulatory frameworks that exist solely to regulate the data broker industry.[4]

This issue brief provides an overview of the emerging state and federal data broker regulatory landscape, focusing on recently enacted laws such as the California Delete Act and the Protecting Americans' Data from Foreign Adversaries Act. It focuses on the evolving legal landscape and shares insights into how laws vary in their key definitions, scope, business obligations, and consumer rights. The laws and regulations analyzed are those that broadly regulate data brokers as a defined category of businesses rather than more general purpose laws that restrict the collection, maintenance, selling, sharing, transferring, or disclosure of personal information even though such requirements necessarily regulate data brokerage. The brief concludes with a look at some of the key ongoing questions and policy considerations for regulating the data broker industry.

Existing Sectoral and Use-Based Regulations

Current attention may be focused on the growing crop of enacted laws and proposed bills that target the data broker industry specifically as a new regulated class, but this industry has long been subject to indirect, sectoral, and use-based regulation. Both the Fair Credit Reporting Act (FCRA) and Section 5 of the FTC Act, for example, have had significant effects upon the industry.

- **FCRA:** Since 1970, the Fair Credit Reporting Act (FCRA) has regulated the creation and use of consumer reports—information communicated by a consumer reporting agency "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general

[1] On April 19, 2023, the House Energy & Commerce Committee's subcommittee on Oversight and Investigations held a hearing titled, *"Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy."* focused on data brokers. Members of Congress continue to scrutinize data brokers. *See also* Press Release, Sen. Elizabeth Warren (D-MA), Warren, Sanders, Wyden, Whitehouse Renew Push to Protect Americans' Sensitive Data From Greedy Brokers (Dec. 10, 2024), https://www.warren.senate.gov/newsroom/press-releases/warren-sanders-wyden-whitehouse-renew-push-to-protect-americans-sensitive-data-from-greedy-brokers; Press Release, Rep. Warren Davidson (R-OH), Reps. Davidson & Biggs Issue Statement on Data Broker Executive Order by the Biden Administration (Feb. 29, 2024), https://davidson.house.gov/press-releases?ID=742CAE5B-C8A2-4186-B7BD-211157EB0505.

[2] *E.g.*, Alfred Ng, *FBI Is Buying Data that Can Be Used to Track People, Patel says*, POLITICO (Mar. 18, 2026), https://www.politico.com/news/2026/03/18/fbi-buying-data-track-people-patel-00834080; Jude Joffe-Block, *Your Data is Everywhere. The Government Is Buying It without a Warrant*, NPR (Mar. 25, 2026) ; Shane Shifflett & Hannah Critchfield, *'We Know You Live Right Here': No Secrets in America's New Surveillance Dragnet*, WSJ (Apr. 30, 2026), https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic.

[3] *E.g.*, Justin Sherman *et al.*, *Data Brokers and the Sale of Data on U.S. Military Personnel* (Nov. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf; Justin Sherman, *Iran War Shows Adversaries Can Exploit Big Data, Too*, LAWFARE (June 22, 2026), https://www.lawfaremedia.org/article/iran-war-shows-adversaries-can-exploit-big-data--too.

[4] Cassandre Coyer, *More States Aim to Rein in, Track Broker Sales of Personal Data*, BLOOMBERG (June 25, 2026), https://news.bloomberglaw.com/privacy-and-data-security/more-states-aim-to-rein-in-track-broker-sales-of-personal-data (discussing data broker–focused bills in 2026).

reputation, personal characteristics, or mode of living" to establish a consumer's eligibility for purposes such as credit, insurance, or employment.[5] This is a use-based restriction that impacts data brokers when they act as a consumer reporting agency or furnish information to a consumer reporting agency. The Consumer Financial Protection Bureau (CFPB) began rulemaking in 2024 to bring data brokers explicitly within the scope of FCRA, but the agency later withdrew the proposed rulemaking.[6]

- **Unfair or Deceptive Trade Practices:** The Federal Trade Commission and state attorneys general have broad authority to bring enforcement actions against companies engaged in unfair or deceptive acts or practices in commerce, including data brokers. These regulators (particularly the FTC) have brought a number of privacy-related enforcement actions against data brokers in recent years for practices such as selling precise geolocation data that reveals consumers' visits to sensitive locations, inadequate notice of data collection and selling, and inadequate security.[7]

Other privacy laws, such as state comprehensive privacy laws and federal sectoral laws such as Title V of the Gramm-Leach-Bliley Act or the Driver's Privacy Protection Act, also regulate data brokers by restricting the collection and use of certain types of personal information.

State Data Broker Laws

At the time of writing, seven U.S. states have enacted standalone data broker laws: Vermont, California, Nevada, Texas, Oregon, Connecticut, and New Jersey.[8] Comparing these laws' definitions, obligations, and consumer rights, a few trends have emerged:

- **Data Brokers Defined Based on Relationship and Activity:** The state data broker laws are scoped to include businesses that collect and sell the personal information of a consumer with whom the business does not have a first-party relationship. There are two key aspects to this scoping. First, these laws are all ***relational*** in that they attempt to regulate only the sale of data collected outside the context of a first-party interaction or a first-party relationship. For example, the state laws typically define a "data broker" as a business that either (1) collects and sells personal data concerning a consumer with whom the business does not have a direct relationship (i.e., not a past or current customer, user, or subscriber), or (2) sells personal data that the business did not collect directly from the consumer. Under some laws, like California's, an entity may still be a data broker if it maintains a direct relationship with the consumer but the data was obtained and sold outside of a first-party interaction where the consumer intended to interact with the business. New Jersey's law also uniquely applies to "data collectors," businesses that have a direct relationship with a

[5] 15 U.S.C. § 1681 *et seq.*
[6] Protecting Americans From Harmful Data Broker Practices (Regulation V); Withdrawal of Proposed Rule, 90 Fed. Reg. 20,568 (May 15, 2025) (withdrawing Protecting Americans From Harmful Data Broker Practices (Regulation V), 89 Fed. Reg. 101,402 (Dec. 13, 2024)).
[7] For more, see Erie Meyer, Stephanie Nguyen & Samuel Levine, Georgetown Institute for Technology Law & Policy, The Data Broker Toolkit: How Enforcers Can Protect Privacy and Stop Data Broker Abuses (Sept. 2025), https://www.law.georgetown.edu/tech-institute/research-insights/insights/the-data-broker-toolkit-2.
[8] In 2026, Connecticut and New Jersey enacted new data broker registration laws and Vermont amended its law. SB 4 & SB 5222, 2026 Reg. Sess., (Conn. 2026); A5328, 2026–27 Reg. Sess., (N.J. 2026); H.211, 2026 Reg. Sess., (Vt. 2026).

consumer but who sell or license personal data to data brokers. Second, these are consumer privacy laws because they focus on ***personal*** information (whether labeled as "personal information," "personal data," "brokered personal data," or "covered information").

- **Registration as a Starting Point:** States have prioritized registration requirements for data brokers thus far. With the exception of Nevada, the state data broker laws all require covered data brokers to register with the state. Although transparency and notice may be prerequisites for consumers to identify data brokers who may maintain information about the consumer, some of these laws do not otherwise provide consumers with enhanced rights such as having their data deleted or opting out of the sale of their data.
- **Inconsistent Public Access to Registries:** As with all technologies, the default settings matter. Of the states that have public registries, they have taken different approaches to consumer access. In Oregon, for example, consumers have to navigate a multistep process with specific search criteria to display a list of registered data brokers. Texas's registry, in contrast, defaults to a list view of all registered data brokers through which an individual can easily scroll.
- **California's One-Stop-Shop Deletion Mechanism:** California has established a first-in-the-nation system to allow consumers to not only identify relevant data brokers but to easily submit deletion requests to data brokers en masse.

This section provides a comparative analysis of the state data broker laws, detailing how their scope, key definitions, and business obligations differ.

What About Daniel's Law?

The laws that are compared in this issue brief were selected for their similarly broad scope: they regulate data brokers as a defined category of businesses and they are consumer privacy laws that broadly apply to the collection and sale of their residents' personal information. For that reason, this section does not discuss Daniel's Law. Originally passed in 2020, Daniel's Law is a New Jersey statute that protects "covered persons"— active, formerly active, or retired judicial officers, law enforcement officers, or child protective investigators, or any immediate family members residing in the same household.[9] A "covered person" can submit a written notice to a business requesting that the business cease disclosing the covered person's "protected information," which includes home address or unpublished home telephone number. The law includes a private right of action and has been a significant source of class action litigation since a 2023 amendment allowed covered persons to assign their claims to third parties.[10] While this law does regulate data brokers, it is not included for comparison because it is narrowly scoped to protect the personal information of only some individuals based on their profession or familial relationship to individuals in covered professions. The laws selected for comparison, in contrast, apply more broadly to the collection and sale of the personal data of any resident of the state.

[9] N.J.S.A. 56:8-166.1.
[10] *Id*. *See also* Kayla Bushey, *US Data Privacy Litigation: Data Brokers and Judicial Privacy Litigation*, IAPP (April 7, 2025), https://iapp.org/resources/article/us-litigation-series-data-brokers-judicial-privacy.

Covered Entities

States have been inconsistent in how they define "data broker." Interpreting "data brokerage" by its broadest possible reading—the buying and selling of data—would extend the term's meaning to cover vast swathes of the economy, particularly if "selling" data includes data sharing for targeted advertising. Under that view, many actors would be labeled a "data broker" even if their primary business model is not trafficking in data. Many businesses "sell" the personal data of consumers with whom they have a direct, first-party relationship but may not consider themselves data brokers. Conversely, interpreting the term narrowly to include only entities whose primary business model is buying and then re-selling consumers' personal data would leave only a small subset of businesses in scope.

States' definitions of "data broker" tend to be ***relational*** in the sense that whether a business is in scope depends on the relationship between the business and the consumer whose personal data is being sold. The specific language varies state-to-state, but four distinct approaches have emerged:

- **Oregon and Connecticut have an exception-based approach** where they (1) define "data broker" broadly as a business that collects and sells personal data, and then (2) provide that a data broker does not include a business that collects information about an individual if that individual is or was in one of several listed relationships with the business. Oregon's exception extends to a business that collects information about a consumer who is or was a "customer, subscriber, or user of the business entity's goods or services." Connecticut's law exempts a business that collects a consumer's information if the consumer is or was "in a contractual relationship with the business." These definitions incorporate a broad concept of a first-party relationship, and hence narrow the laws' reaches, because any past or present first-party, commercial relationship between the consumer and the business is enough to trigger the exception regardless of the specific context in which the business actually collected the relevant data.
- **New Jersey is unique in requiring "data collectors" to register annually.** New Jersey's definition of "data broker" is similar to that in Oregon and Connecticut—it excludes businesses that have a "direct relationship" with the consumer which includes past or present customers, subscribers, or users. However, New Jersey's law uniquely requires "data collectors"—businesses that have a direct relationship with a consumer and sell or license the consumer's personal data to a data broker—to register as well. This expands the law's reach significantly.
- **California and Vermont offer a more contextual approach**, focusing on whether a consumer was intentionally interacting with the business when the personal information was collected. The California Delete Act defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a ***direct relationship***." The law's implementing regulations clarify that a direct relationship requires a consumer to intentionally interact with the business, and "[a] business is still a data broker and does not have a direct relationship with a consumer as to personal information it sells about the consumer that it collected outside of a 'first party' interaction with the consumer." Vermont amended its law in 2026 to align with California's contextual definition of "direct relationship." Previously, Vermont had an exception-based definition similar to that in Oregon and Connecticut.
- **Texas has taken a different approach by defining a data broker** as a business that collects, processes, or transfers personal data that it did not ***collect directly*** from the individual. This definition is focused on the ***specific interaction*** in which the data was collected rather than the

broader relationship between the business and individual. Texas's definition may therefore be closest in practice to California's and Vermont's definitions.

- **Nevada presents the narrowest definition**, only covering businesses whose ***primary business*** is ***purchasing and selling*** covered information about consumers with whom the business ***does not have a direct relationship***.

The following table includes relevant definitions from each law:

State	Definition of "Data Broker"
California **(Delete Act)**	"Data broker" means a business [under the CCPA] that knowingly collects and sells to third parties the personal information of ***a consumer with whom the business does not have a direct relationship***.[11] "Direct relationship" means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services. . . . A business does not have a "direct relationship" with a consumer simply because it collects personal information directly from the consumer; ***the consumer must intend to interact with the business.*** A business is still a data broker and does not have a direct relationship with a consumer as to personal information it sells about the consumer that it collected outside of a "first party" interaction with the consumer, as that term is defined in California Code of Regulations, title 11, section 7001.[12]
Connecticut	"Data broker" means any business or, if such business is not an individual, any portion of such business that sells or licenses brokered personal data to another person; The provisions of sections 1 to 10, inclusive, of this act shall not apply to: . . . a business that collects information concerning a consumer if the consumer is or was (A) ***in a contractual relationship with the business***, (B) an investor in the business, (C) a donor to the business, or (D) in any relationship with the business that is similar to the relationships described in subparagraphs (A) to (C), inclusive, of this subdivision;[13]
Nevada	"Data broker" means a person whose primary business is purchasing covered information about consumers with whom the person does not have a direct relationship and who reside in this State from operators or other data brokers and making sales of such covered information.[14]
New Jersey	"Data broker" means a person or legal entity, including, but not limited to, a controller, that knowingly collects or purchases the personal data of a consumer with whom the person or legal entity does not have a ***direct relationship*** and sells or licenses that data to a third party. A third party shall not include a processor if licensure or disclosure of personal data to the processor is solely to process the personal data on the data broker's or data controller's behalf. . . . Examples of a direct relationship include if the consumer is a ***past or present: (1) customer, client, subscriber, or user*** of the person or legal entity's goods or services; (2) employee, contractor, or agent of the person or legal entity; (3) investor in the person or legal entity; or (4) donor to the person or legal entity. **"Data collector"** means a business, or units of a business, separately or together, that knowingly: (1) collect the personal data of a consumer with whom the data collector has a direct relationship; and (2) sell or license such personal data to a data broker.[15]

[11] Delete Act. Cal. Civ. Code § 1798.99.80, subd. (c) (emphasis added).
[12] Cal. Code Reg. tit. 11, § 7601, subd. (d).
[13] S.B. 4, 2026 Reg. Sess., §§ 1 & 7 (Conn. 2026).
[14] Nev. Rev. Stat. § 603A.323.
[15] A5328, 2026–27 Reg. Sess., (N.J. 2026).

State	Definition of "Data Broker"
Oregon	(A) "Data broker" means a business entity or part of a business entity that collects and sells or licenses brokered personal data to another person. (B) "Data broker" does not include: . . . (iii) A business entity that collects information about a resident individual if the resident individual is or was: (I) ***A customer, subscriber or user of the business entity's goods or services***; (II) An employee or agent of the business entity or is in a contractual relationship with the business entity; (III) An investor in the business entity; (IV) A donor to the business entity; or (V) In another relationship with the business entity the nature of which is similar to the relationships described in this sub-subparagraph;[16]
Texas	"Data broker" means a business entity that collects, processes, or transfers personal data that the business entity ***did not collect directly from the individual*** linked or linkable to the data.[17]
Vermont	(6) (A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. (B) As used in this subdivision (6), "direct relationship" means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services. A consumer does not have a direct relationship with a business if the purpose of the consumer's engagement is to exercise a consumer right or for the business to verify the consumer's identity. A business does not have a direct relationship with a consumer simply because the business collects brokered personal information directly from the consumer; the consumer must intend to interact with the business. A business is still a data broker and does not have a direct relationship with a consumer as to the brokered personal information the business sells about the consumer that it collected outside of a first-party interaction with the consumer.[18]

Each of these definitions has additional nuance that is not fully explored in this issue brief, such as Nevada's narrow focus on entities that ***purchase*** and sell covered information or the bounds of Connecticut's exception for consumers with a "contractual" relationship with the business.

Several of these state laws include additional qualifiers and entity-level exemptions. For example, Texas's law includes revenue and processing thresholds to limit application to small businesses in addition to broad carve-outs for service providers, entities collecting data from other entities in common ownership, governmental entities, congressional designated nonprofits and similar organizations, consumer reporting agencies insofar as they are engaging in FCRA-regulated activity, and GLBA-covered financial institutions.

[16] Or. Rev. Stat. § 646A.593.
[17] Tex. Bus. & Prof. Code § 510.001(4).
[18] Act 138, H.211, 2026 Reg. Sess. (Vt. 2026) (amending Vt. Stat. Ann. tit. 9 § 2430) (effective January 1, 2027).

California's Delete Act includes exemptions for entities covered by FCRA, GLBA, the California Insurance Information and Privacy Protection Act, and covered entities or business associates to the extent their processing is exempt under the CCPA. Oregon's law likewise exempts governmental agencies, GLBA-covered financial institutions, and consumer reporting agencies engaged in FCRA-covered activities.

Covered Information

States have taken two distinct approaches to defining what data is in scope. Oregon and Connecticut have narrow definitions covering listed data elements about an individual if those elements are categorized or organized for sale or licensing to another person.[19] The listed data elements are common identifiers such as name, address, date of birth, biometric data, and social security number. California, Texas, Vermont (after the 2026 amendments), and New Jersey have taken a broader approach, including definitions of personal information or personal data akin to those under comprehensive privacy laws—any information that is linked or reasonably linkable to an identified or identifiable individual.

State	Definition of Covered Information
California	(1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: [Full list omitted; Notable items include identifiers, commercial information, internet or other electronic network activity information, professional or employment-related information, and inferences.] (2) (A) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. . . . (3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.[20]
Connecticut	"Brokered personal data" means one or more of the following personal data elements concerning a consumer, if categorized or organized for sale or license to a third party: (A) Name; (B) address; (C) date of birth; (D) place of birth; (E) mother's maiden name; (F) unique biometric data (i) generated from measurement or technical analysis of a human body characteristic, including, but not limited to, a fingerprint, retina or iris image or other unique physical or digital representation of biometric data, and (ii) used by the owner or licensee of such unique biometric data to identify or authenticate the consumer; (G) name or address of a member of the consumer's immediate family or household; (H) Social Security number or other government-issued identification number; or (I) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the

[19] Connecticut's new law is inconsistently scoped with respect to covered information. The definition of "data broker" is tied to the sale of "brokered personal data," which follows the Oregon approach of listed data elements if categorized or organized for sale to a third party. However, the obligation for data brokers to comply with a verified deletion request provides that a data broker must "delete any ***personal data*** such registered data broker maintains concerning the participating consumer." The law defines "personal data" consistently with the Connecticut Data Privacy Act (CTDPA) as "any information that is linked or reasonably linkable to an identified or identifiable individual." Thus, the data that a data broker must delete pursuant to a deletion request may be broader than the data that brings a data broker within the scope of the law. *See* S.B. 4, 2026 Reg. Sess., § 1 (Conn. 2026).

[20] Cal. Civ. Code § 1798.140, subd. (v); Cal. Civ. Code § 1798.99.80, subd. (a) (providing that the definitions of the CCPA apply to the Delete Act unless otherwise specified).

State	Definition of Covered Information
	consumer with reasonable certainty; "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;[21]
Nevada	"Covered information" means any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator or a data broker in an accessible form: 1. A first and last name. 2. A home or other physical address which includes the name of a street and the name of a city or town. 3. An electronic mail address. 4. A telephone number. 5. A social security number. 6. An identifier that allows a specific person to be contacted either physically or online. 7. Any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator or data broker in combination with an identifier in a form that makes the information personally identifiable.[22]
New Jersey	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable person. "Personal data" shall not include de-identified data or publicly available information.[23]
Oregon	"Brokered personal data" means any of the following computerized data elements about a resident individual, if categorized or organized for sale or licensing to another person: (A) The resident individual's name or the name of a member of the resident individual's immediate family or household; (B) The resident individual's address or an address for a member of the resident individual's immediate family or household; (C) The resident individual's date or place of birth; (D) The maiden name of the resident individual's mother; (E) Biometric information about the resident individual; (F) The resident individual's Social Security number or the number of any other government-issued identification for the resident individual; or (G) Other information that, alone or in combination with other information that is sold or licensed, can

[21] S.B. 4, 2026 Reg. Sess., § 1 (Conn. 2026).
[22] Nev. Rev. Stat. § 603A.320.
[23] A5328, 2026–27 Reg. Sess., (N.J. 2026).

State	Definition of Covered Information
	reasonably be associated with the resident individual.[24]
Texas	"Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the information is used by a controller or processor in conjunction with additional information that reasonably links the information to an identified or identifiable individual. The term does not include deidentified data, employee data, or publicly available information.[25]
Vermont	(A) "Brokered personal information" means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one of more identified or identifiable individuals. (B) "Brokered personal information" does not include publicly available information.[26]

These laws consistently exempt publicly available information, although neither Nevada nor Oregon define the term.[27] Connecticut defines "publicly available information" to exclude information such as consumer profiles created from collating and combining government records or used to generate inferences. Connecticut's definition therefore narrows the publicly available information exception and broadens the law's reach. States have also included data-level exemptions. For example, Texas's law does not apply to data subject to GLBA.

Registration and Business Obligations

States tend to impose a number of business obligations on covered data brokers, including registering with the state and maintaining adequate information security. These requirements are not consistent across the state laws. Nevada's law, for example, is both narrow in its scope and its obligations: it does not require data brokers to register with the state, but it does allow consumers to submit a verified request to a data broker (defined narrowly) to opt-out of having their covered information sold. This section provides an overview of the common requirements amongst the more prescriptive data broker laws in California, Connecticut, Oregon, New Jersey, Texas, and Vermont.

Registration. California, Connecticut, Oregon, New Jersey, Texas, and Vermont all require data brokers to register with the state annually. This process typically requires the data broker to file a registration statement or application with a specified government agency or official (e.g., secretary of state) and pay a registration fee. New Jersey's law is unique in both its scope and cost. As discussed above, New Jersey also requires "data collectors"—businesses that have a direct relationship with a consumer and sell the consumer's personal data to a data broker—to register. New Jersey also has a range of registration fees that are based on the number of consumers whose personal data a data broker or data collector collects

[24] Or. Rev. Stat. § 646A.593.
[25] Tex. Bus. & Prof. Code § 510.001(11).
[26] Act 138, H.211, 2026 Reg. Sess. (Vt. 2026) (amending Vt. Stat. Ann. tit. 9 § 2430) (effective January 1, 2027).
[27] Both of these states' laws appear to distinguish between "publicly available information" and "information that is lawfully available from federal, state or local government records" whereas many other state laws define publicly available information to include such government records.

and sells or licenses. New Jersey's lowest fee tier is $5,000 for fewer than 100,000 affected consumers, and the highest tier is $1,500,000 for more than 4.5 million affected consumers. In the other states, registration fees range from $100 to $6,000.

Each state requires different information at registration. While most require basic descriptive information about the data broker, such as legal name and contact information, states also require disclosures about the company's data collection and sharing practices. For example, California requires detailed disclosures as to whether a data broker collects—

- Names, dates of birth, ZIP codes, email addresses, or phone numbers;
- Account logins or account numbers in combination with information (security or access code or password) that would permit access to a consumer's account with a third party;
- Government-issued identification numbers (drivers' license, state ID, tax ID, SSN, passport, military ID, or other);
- Mobile advertising ID numbers (MAID), connected TV ID numbers, or vehicle identification numbers (VIN);
- Citizenship data (including immigration status);
- Union membership status;
- Sexual orientation status;
- Gender identity and gender expression data;
- Biometric data;
- Precise geolocation;
- Reproductive health care data; or
- If the data broker collects none of the above, it must identify one to three of the most common types of personal data that the data broker collects.

California also requires data brokers to disclose whether they have shared or sold consumers' personal data in the last year to a/the—

- Foreign actor;
- Federal government;
- State government;
- Law enforcement (unless pursuant to a subpoena or court order); or
- Developer of a GenAI system or model.

Registration and Registries

All of these state laws, except for Nevada's, require data brokers to register annually with the state. Public access to these registries remains inconsistent across the state laws. In Oregon, for example, consumers have to navigate a multistep process with specific search criteria to display a list of registered data brokers. Texas's registry, in contrast, defaults to a list view of all registered data brokers through which an individual can easily scroll or search based on a variety of criteria, including registration number, legal name, address, website, or category of data processed. States that have searchable registries may also make available to the public information from data brokers' registration forms (e.g., contact information and disclosures about

the categories of data that the data broker collects). Vermont's 2026 amendment to its law will improve individuals' access to its registry by creating a downloadable spreadsheet of registered data brokers.

Data Security. In addition to registration requirements, the laws in Texas and Vermont require data brokers to maintain adequate data security.[28] Vermont's law subjects data brokers to a duty to protect "personally identifiable information" (a distinct—and narrower—term than "brokered personal information"). Texas's law likewise requires data brokers to protect "personal data," and the requirements in both laws are substantially similar.

These laws require data brokers to develop, implement, and maintain a comprehensive information security program. Such programs must include administrative, technical, and physical safeguards that are appropriate to the business's size, scope, and type, the amount of resources available to the data broker, the amount of stored data, and the need for security and confidentiality of covered data. These requirements correlate to data security requirements under other privacy and security laws, and both laws require that any safeguards adopted are consistent with safeguards for covered data and information set forth in other state and federal regulations applicable to the data broker. Both laws detail specific components that must be included in a comprehensive information security program, such as regular monitoring of program performance and review of security measures. These laws also identify required security components, to the extent technically feasible, such as secure user authentication protocols, secure access control measures, encryption of data stored on portable devices, up-to-date firewall protection and operating system security patches, and education and training for employees.

Other Requirements. Vermont's law, as originally enacted, included two unique prohibitions. A person may not: acquire brokered personal information through "fraudulent means"; or acquire or use brokered personal information for stalking or harassing another person, committing a fraud (including identity theft, financial fraud, or e-mail fraud), or engaging in unlawful discrimination (including in employment and housing).[29] Note that these prohibitions are not limited to data brokers, instead applying more broadly to "a person," but they are limited to the acquisition or use of "brokered personal information." The law does not define "fraudulent means," but the Attorney General's guidance provides that "[t]he concepts of fraud, stalking and harassing, identity theft, and unlawful discrimination are addressed in the common law and other statutes."[30]

Vermont's 2026 update to its law brought new requirements as well. Notably, the law now imposes due diligence or "know your customers"–style requirements prior to disclosing brokered personal information, such as: requiring "prospective users" of brokered personal information to identify themselves, state their purposes for seeking the information, and certifying that the information will not be used for other purposes; and, prior to disclosing such information, verifying the prospective user's identity, reviewing the stated purposes for using the information, and not disclosing the information where there are "reasonable

[28] While this section covers only data security obligations specific to data brokers under these state laws, data brokers in each of these states may be subject to additional data security obligations, including those under comprehensive consumer privacy laws in effect in California, Connecticut, Oregon, and Texas.
[29] Vt. Stat. Ann. tit. 9 § 2431.
[30] Guidance on Vermont's Act 171 of 2018: Data Broker Regulation, Vt. Off. of the Att'y Gen., (Dec. 11, 2018).

grounds for believing that the information will be used to violate State or federal law or will not be used for the purposes stated by the user."[31]

New Jersey's law prohibits data brokers or data collectors from selling or licensing sensitive data. "Sensitive data" and "sale" are defined consistently with the state's comprehensive privacy law, whereas "license" is undefined.[32]

Accessible Deletion Mechanisms and Third-Party Audits

Privacy proponents often suggest that one of the challenges consumers face in a control- or rights-based model of privacy law is that it is difficult to exercise consumer rights at scale. While a law may give a consumer the right to have a business delete their personal data upon the consumer's request, that consumer has many commercial relationships and may not have the time or capacity to exercise that right comprehensively on a company-by-company basis. This problem is especially acute when it comes to exercising rights with respect to data brokers because there often is no first-party relationship, adding more friction to the process. Maintaining public registries can ease that burden by providing an accessible list of relevant data brokers, but consumers still must expend considerable effort to submit rights requests to multiple entities.

California changed this paradigm in 2023 when it enacted the Delete Act. In addition to updating the state's data broker registration requirements, it required the California Privacy Protection Agency (CalPrivacy) to, by January 1, 2026, establish "an accessible deletion mechanism" that "implements and maintains reasonable security procedures and practices" and allows a consumer to submit a single, verifiable deletion request to as many registered data brokers in the system as the consumer desires. The statute lays out additional criteria for how the system should function, which CalPrivacy has further fleshed out through rulemaking. Consumers can create an account with the agency to access the DROP system, using an identity verification procedure. After registering, consumers are able to input information about themselves that align with data types that data brokers may possess (e.g., names, addresses, email addresses, MAIDs). Building such a database of consumer information poses its own privacy and security risks. To compensate for that security risk, and to enable more secure data matching between consumer requests and relevant data brokers, all personal information inputted by consumers is hashed. Consumers are then able to review a list of registered data brokers and select which brokers they want to delete their personal information. The DROP system opened to Californians on January 1, 2026.

Data brokers, too, must create a DROP account. Registered data brokers must select relevant consumer deletion lists that correspond to consumer identifier(s) that match to personal information about consumers that the data broker maintains. Starting on August 1, 2026, data brokers must begin complying with deletion requests submitted via the DROP system. The regulations include lengthy technical procedures for this process, as well as nuanced exceptions. To summarize the process, data brokers must access the DROP system (either manually or through an automated process, as facilitated by the agency), download relevant consumer deletion lists, standardize their own personal information records in accordance with

[31] Act 138, H.211, 2026 Reg. Sess. (Vt. 2026) (amending Vt. Stat. Ann. tit. 9 § 2430) (effective January 1, 2027).
[32] A5328, 2026–27 Reg. Sess., § 2(a) (N.J. 2026). The definition of "sale" in the data broker law is slightly broader than under the comprehensive privacy law, as it lacks several of the common exceptions (e.g., disclosures in a merger or acquisition).

the regulations,[33] use the same hashing algorithm provided in the consumer deletion list on the data brokers' own records (after standardizing), and delete the matching data. Data brokers will be required to repeat this process regularly in 45 day intervals.

The deletion right is not absolute. A data broker is not required to comply with a deletion request if certain exceptions from the CCPA apply—either (1) maintaining the personal information is "reasonably necessary" for a purpose under Cal. Civ. Code § 1798.105, subdivision (d), or (2) deletion is not required under Cal. Civ. Code §§ 1798.145 or 1798.146.[34] The first exception applies where it is "reasonably necessary" for the business to maintain the personal information for one of several listed purposes, including:

- Completing the transaction for which the personal information was collected;
- **Providing a good or service either "requested by the consumer" or "reasonably anticipated by the consumer** within the context of a business' ongoing business relationship with the consumer";
- **Performing a contract between the business and the consumer;**
- Helping to ensure secure security and integrity (to the extent "reasonably necessary and proportionate");
- Debugging to identify and repair errors that impair existing intended functionality;
- Engaging in public or peer-reviewed scientific, historical, or statistical research that meets specified ethics and privacy safeguards, including informed consent; and
- Enabling "solely internal uses" reasonably aligned with a consumer's expectations based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information;
- Complying with a legal obligation; and more.[35]

The second set of exceptions—Cal. Civ. Code §§ 1798.145 or 1798.146—are the CCPA's general exceptions, limitations, and data-level exemptions.

At the time of writing, the DROP system is open to Californians to register and submit requests, but data brokers are not yet required to comply with these requests. The Delete Act's implementations can be broken down into distinct phases. Initially, the existing data broker registry was transferred to CalPrivacy, which then conducted initial rulemaking under the law. Currently, CalPrivacy is engaged in the rollout of the DROP system. The system opened to Californians on January 1, 2026, and data brokers must begin complying with requests on August 1, 2026. Another key milestone will be January 1, 2028, as data brokers will have an additional obligation to undergo independent third-party audits to determine their compliance with the law. These audits will need to be conducted every three years. A data broker must submit an audit report and any related materials to CalPrivacy within 5 business days of a written request from the agency. Reports and related materials must be maintained for at least six years. In CalPrivacy's November 2025 Board Meeting, it was indicated that the agency could conduct rulemaking to clarify the audit requirements prior to that January 1, 2028 effective date.

Connecticut became the second state to enact a Delete Act when the Governor signed SB 4 on May 27. Connecticut's law closely resembles California's, including aspects such as third-party audits of data

[33] This process involves steps such as using all lowercase letters, removing extraneous or special characters except for non-English language characters and email addresses, and formatting date of birth in a specified manner.
[34] Cal. Civ. Code § 1798.99.86, subd. (c)(2).
[35] Cal. Civ. Code § 1798.105, subd. (d).

brokers' compliance with the law. These new requirements for data brokers have staggered effective dates: Data brokers must begin registering with the state on January 1, 2027. The Commissioner of Consumer Protection must establish an accessible deletion mechanism by July 1, 2028. Data brokers will have to begin complying with deletion requests submitted via the accessible deletion mechanism on October 1, 2028. These staggered dates will allow for necessary rulemaking and technical implementation.

It remains to be seen what potential challenges consumers, data brokers, and the state will face as an accessible deletion mechanism comes online.[36] Nevertheless, California's DROP serves as proof-of-concept. Now that one state (soon to be two) has such a mechanism in place, it is more likely that the concept will appear in future state and federal regulatory efforts.

Comprehensive Privacy Laws

The focus of this issue brief is emerging regulation in the U.S. narrowly scoped to the data broker industry—not broadly applicable consumer protection or privacy laws. Nevertheless, these laws can have a significant impact on the data broker industry. Comprehensive consumer privacy laws, for example, directly regulate data brokers if they meet relevant thresholds to be within scope. These laws provide consumers with rights to have their personal data deleted, opt-out of having their personal data sold, and laws like Maryland's impose substantive data minimization requirements limiting the collection of personal data to what is reasonably necessary to provide a requested product or service. These obligations also have downstream consequences for data brokers when they impact other businesses' ability to sell personal data. Two prominent enforcement actions, for example, both concerned allegations that controllers were selling personal data to data brokers in violation of the law.

- **Enforcement Actions:** Texas announced the first lawsuit under a state comprehensive privacy law when it sued insurer Allstate and the company's data broker subsidiaries (Arity) in 2025. In the complaint, Texas AG Paxton alleged that the companies were collecting consumers' driving data (including precise geolocation data) via a software development kit that app developers were paid to integrate into their apps. That SDK data was then combined with personal data licensed from app developers to identify the individual whose data was being collected, and the data was subsequently used for insurance purposes. The complaint further alleged that Arity (a subsidiary of Allstate) was required to register as a data broker—because it was deriving revenue from the processing and transferring of personal data that it did not collect directly from the individuals—but failed to do so. This action illustrates how a company's data sharing with a data broker, even a subsidiary, can subject them to regulatory scrutiny. California settled a similar case concerning connected cars and the use of driving data in May 2026, resulting in a record $12.75 million civil penalty. In that case, regulators alleged that GM was selling consumers' personal information—including names, contact information, location data, and driving data collected via the OnStar service—to data brokers for use in insurance in violation of the CCPA's purpose limitation and data minimization requirements.

[36] For an early assessment of compliance with California's Delete Act, see Anna-Maria Gueorguieva, *Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law*, FAccT '26, available at https://doi.org/10.48550/arXiv.2605.21376.

- **Legislative Trends Towards Banning Sale of Sensitive Data (Including Precise Geolocation Data):** Another trend likely to have significant downstream consequences for the data brokerage industry is the growing number of states ***banning*** the sale of certain types of personal data. In 2024, Maryland became the first U.S. state to ban the sale of sensitive data in a comprehensive privacy law.[37] Others have since followed suit. In 2025, Oregon banned the sale of precise geolocation data and personal data of consumers under 16.[38] In 2026, Virginia and Connecticut banned the sale of precise geolocation data, New Hampshire banned the sale of children's personal data, and New Jersey banned the sale of sensitive data.[39] The consequences of these bans remain to be seen. The unrestricted sale of sensitive data poses considerable risk to individuals.[40] Nevertheless, such bans—particularly for the sale of location data—could disrupt lower risk, socially beneficial services, such as non-law enforcement government uses (e.g., traffic analysis, emergency response services, disaster prevention and relief) and business planning and analytics apart from targeted advertising. As these types of restrictions are considered, policymakers should consult stakeholders on these restrictions' practical implications, and continue that dialogue in states that have already passed them, to assess real-world effects and revisit as needed.

Federal Data Broker Regulation

In addition to these new state laws, data brokers are also subject to regulatory scrutiny at the federal level. Although there is no federal data broker registry law comparable to the state laws profiled above, data brokers have been the target of legislation, rulemaking, and enforcement activity. The Protecting Americans' Data from Foreign Adversaries Act of 2024, for example, prohibits data brokers from making Americans' sensitive data available to foreign adversaries. The Consumer Financial Protection Bureau initiated, but did not complete, rulemaking that would have brought data brokers within scope of the Fair Credit Reporting Act, and the Department of Justice finalized a regulation on the transfer of bulk sensitive data to countries of concern in 2024. Apart from new laws and regulations, data brokers have also been a regular target for enforcement under existing consumer protection laws. The Federal Trade Commission has settled several enforcement actions with data brokers in recent years, most of which concerned the collection and sharing of precise geolocation data connected to sensitive locations.

Protecting Americans' Data from Foreign Adversaries Act

The Protecting Americans' Data from Foreign Adversaries Act (PADFAA) was enacted in April 2024 as part of a foreign aid package (H.R. 815) that also included the more publicized Protecting Americans from Foreign Adversary Controlled Applications Act. The law prohibits data brokers from making personally identifiable sensitive data of U.S. individuals available to any foreign adversary country (North Korea, China,

[37] Md. Code Ann. Com. Law § 14–4707(a)(2).
[38] Or. Rev. Stat. § 646A.578(2)(d).
[39] S.B. 338, 2026 Reg. Sess., (Va. 2026); S.B. 4, 2026 Reg. Sess., (Conn. 2026); HB 1460, 2026 Reg. Sess., (N.H. 2026); A5328, 2026–27 Reg. Sess., (N.J. 2026) (applying more broadly than other requirements under the law)..
[40] *E.g.*, The Associated Press, *Priest Outed Via Grindr App Highlights Rampant Data Tracking*, NBC NEWS (July 22, 2021), https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493.

Russia, and Iran) or an entity controlled by a foreign adversary. PADFAA's key terms differ from those common under the state data broker laws.

"Data broker" is defined as an entity that, "***for valuable consideration***, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals, that the entity ***did not collect directly*** from such individuals, to another entity that is not acting as a service provider." The term is subject to enumerated exemptions, including for transmitting data at the request of an individual and for reporting and publishing news. An entity is not a data broker if it is acting as a "service provider." This definition is closest to that under Texas's law, as it focuses on whether the data was collected "directly" from the individual, regardless of whether the entity otherwise has a first-party relationship with the individual.

The term ***"personally identifiable sensitive data"*** is broader than one may expect from its plain meaning. This is defined as ***any sensitive data*** that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to an individual. The "linked or reasonably linkable" standard resembles the broad definitions of personal information or personal data under state comprehensive privacy laws. Sensitive data, in turn, is defined broadly. There are sixteen enumerated categories and a catch-all for any data that a data broker makes available to a foreign adversary country or entity controlled by a foreign adversary for the purpose of identifying the types of data in the sixteen enumerated categories. These categories include:

- Government-issued identifiers;
- Information revealing health conditions and treatment;
- Biometric information;
- Genetic information;
- Precise geolocation information;
- An individual's private communications, information identifying parties to such communications, or information pertaining to the transmission of such communications;
- Account or device log-in credentials or codes;
- Information identifying sexual behavior;
- Calendar information;
- A photo or video showing a naked or undergarment-clad private area;
- Information revealing video content requested by an individual;
- Information about an individual under the age of 17;
- An individual's race, color, ethnicity, or religion;
- ***Information identifying an individual's online activities over time and across websites or online services;*** and
- Information revealing an individual's status as a member of the Armed Forces.

These categories go beyond what is typically included as "sensitive data" under state privacy laws, and including information that identifies activities over time and across websites or online services likely brings in scope targeted advertising.

The Federal Trade Commission enforces violations of PADFAA as violations of a trade regulation rule under the FTC Act, which can carry significant civil penalties (currently up to $53,088 per violation, subject to

regular adjustment). While the FTC has not yet initiated formal enforcement actions, the agency warned 13 data brokers in February 2026 that they must comply with the law.

Department of Justice Bulk Sensitive Data Transfer Rule

PADFAA was enacted a mere two months after President Biden signed Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." Based on a perceived national security risk that countries of concern could "analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States," the EO directed the Attorney General to issue regulations on U.S. persons engaging in transactions involving bulk U.S. sensitive personal data. The DOJ finalized this rule (28 C.F.R. Part 202) ("the Rule") in January 2025 and it is currently in effect. Data brokers are within scope of the Rule, as there are specific restrictions on "data brokerage" as a defined activity, but the rule applies more broadly than to data brokers alone.

The Rule regulates the transfer of bulk U.S. sensitive personal data to a "country of concern" or "covered person." Key terms:

- **Sensitive Personal Data:** Covered personal identifiers, precise geolocation data, biometric identifiers, human `omic data, personal health data, personal financial data, or any combination thereof.
- **Bulk:** Any amount of sensitive personal data that meets or exceeds thresholds under the Rule at any point in the preceding 12 months, whether through a single transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person. Thresholds are data collected about or maintained on more than either: 100 U.S. persons, 1,000 U.S. persons, 10,000 U.S. persons, or 100,000 U.S. persons, depending on the data type.
- **Bulk U.S. sensitive personal data:** A collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set in the definition of "bulk."
- **Country of Concern:** China (including Hong Kong and Macao), Cuba, Iran, North Korea, Russia, and Venezuela. This is a distinct but overlapping term as compared to "foreign adversary" used in PADFAA.
- **Covered Person:** Persons and entities with sufficient connections to a country of concern, including based on ownership, residency, employment, or determination by the Attorney General.

Under the Rule, two categories of transactions are ***prohibited*** and three other categories are ***restricted***. One of the prohibited transactions is any U.S. person engaging in a covered data transaction involving ***data brokerage*** with a country of concern or covered person. Data brokerage is defined as the sale or licensing of access to data, or similar transaction, involving the transfer of data from a provider to a recipient where the recipient did not collect or process the data directly from the individuals linked or reasonably linkable to the collected or processed data, subject to exceptions. There are additional data brokerage requirements designed to

prevent downstream resale or transfer of data through third parties: no U.S. person can knowingly engage in any transaction with a foreign person that is not a covered person, if that transaction involves data brokerage and any access by a foreign person to government-related data or bulk U.S. sensitive personal data, unless the U.S. person contractually obligates the recipient from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person and the U.S. person reports any known or suspected violations by the recipient as required under the Rule.

Recent FTC Enforcement Under Section 5

Between the agency's enforcement powers under the Fair Credit Reporting Act and Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce, data brokers have long been subject to enforcement actions brought by the Federal Trade Commission (FTC). During Lina Khan's tenure as Chair, however, the agency brought a flurry of enforcement actions against companies operating in the mobile data, location analytics, and advertising technology ecosystem. Between 2022 and 2024, the FTC announced enforcement actions against companies Kochava, X-Mode Social, InMarket Media, Mobilewalla, and Gravy Analytics.[41] In each enforcement action, the FTC alleged that the company collected and sold consumers' personal data or inferences generated therefrom without adequate notice or consent. Furthermore, the data in question often included sensitive data, such as precise geolocation data and location data that revealed other sensitive characteristics about a consumer (e.g., religion or sexual orientation).

One consistent thread across these cases was a focus on precise geolocation data that is associated with a consumer's presence in a sensitive location. In addition to other injunctive terms, all five of these settlements restrict the defendant from selling "sensitive location data." This term has been consistently defined as location data (within 1,850 feet) associated with a sensitive location, which is a defined term with enumerated categories. Looking at the Mobilewalla order, for example, sensitive location included:

(1) Medical facilities (with a lengthy list of examples);
(2) Religious organizations;
(3) Correctional facilities;
(4) Labor union offices;
(5) Locations held out to the public as predominantly providing education or childcare services to minors;
(6) Locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife;
(7) Locations held out to the public as predominantly providing services based on racial or ethnic origin;
(8) Locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants;
(9) Locations of public gatherings of individuals during political or social demonstrations, marches, and protests; or

[41] Other cases, such as those against Avast and General Motors, included claims alleging unlawful data sharing with data brokers or consumer reporting agencies.

(10) Military installations, offices, or buildings.

The Kochava case is a slight outlier. Although that action was the first to be initiated from this group, it did not settle until May 2026 after four years of litigation. The settlement includes a slightly narrower definition of "sensitive location," omitting items (3), (4), (6), (7), (9), and narrowing (8) to exclude references to refugees or immigrants. The prohibition on sale is also weaker in that settlement, as the prohibition on selling sensitive location data does not apply if the company has a "direct relationship" with the consumer, the consumer has provided affirmative express consent, and the sensitive location data "is used to provide a service directly requested by the consumer."

It remains to be seen whether the current or a future FTC will continue these trends or further evolve the agency's theories of harm with respect to data brokerage.

Policy Considerations

As the data broker regulatory landscape continues to evolve, policymakers will have to address important questions related to the scope and purpose of these frameworks. FPF hosted a roundtable discussion on data brokerage in May 2026 with participants from civil society, industry, and academia to foster dialogue between a diverse group of stakeholders with differing perspectives on the harms and benefits of data brokerage. The discussion in that roundtable—in addition to other conversations with key stakeholders and observations on public discourse around data brokerage—illuminated several issues that are critical to developing effective regulatory frameworks but currently lack agreement across stakeholders.

These topics include the entities and data that should be **in scope** of new regulations, whether regulations should be "one-size-fits-all" or tailored to proscribe specific harmful **use cases**, how to ensure that beneficial uses are not unintentionally impeded, and how existing legal and technical **safeguards** either mitigate the need for new regulatory frameworks or could inform the content of new requirements. This section concludes with a reflection on the trust deficit that has emerged between civil society, industry, consumers, and policymakers regarding data brokerage, and the fact that this deficit may be contributing to the current fractured policy environment. Adoption of voluntary practices by industry actors and a commitment to sustained, productive dialogue by policymakers, civil society, and industry alike can support evidence-based policymaking that addresses risks and enables benefits.

Scoping: Types of Data and Entities Subject to Regulations

Policymakers must decide what **types of data** should be in scope of new regulations and whether different obligations should attach to different types of data or to different contexts in which such data is used. State comprehensive privacy laws have typically included distinctions between publicly available information, personal data in an employment or business-to-business context, and personal data in the individual or household context. Privacy laws also often include heightened protections for uses of sensitive data (e.g., precise geolocation data, health data, personal data of a known child). Data broker regulations also engage in such line-drawing, but reaching consensus on the best approach is and will continue to be difficult.

From the perspective of privacy advocates, broad exclusions for certain data types may undermine regulations' efficacy, especially as artificial intelligence improves the ability to make sensitive inferences about individuals from non-sensitive data. Industry stakeholders may instead see broad restrictions on the sale of sensitive data as insufficiently tailored to specific harmful use cases. Balancing both considerations will be necessary to create a workable framework. Existing state comprehensive privacy laws demonstrate the feasibility of a risk-based approach that broadly regulates consumer data while both exempting data subject to other laws and providing heightened protections such as informed consent for uses of sensitive data. Policymakers should also keep in mind that new regulations may be subject to First Amendment challenges, particularly if the sharing of publicly available information is restricted.[42]

Another significant challenge in scoping data broker regulations is determining what kind of commercial activity makes a business a "data broker." As detailed above, the current state data broker registration laws each attempt to limit their scope to businesses that have a certain type of **indirect relationship** with the individuals whose data are being sold. Despite the conceptual similarity of these laws' approaches, the laws have taken divergent approaches to defining the scope of activities subject to regulation. The breadth of these different approaches present unique trade-offs.

A **narrow** definition of a data broker would be limited to entities that lack any relationship to a consumer whose personal data they collect and sell. Nevada's definition is closest to this because its scope is limited to businesses whose primary business is ***purchasing and selling*** covered information about consumers with whom the business ***does not have a direct relationship***. This creates two layers of distance: between the consumer and the transaction itself, and between the consumer and the business. A slightly broader approach would include entities that sell personal data from consumers with whom they lack a specified relationship , even if it is not their primary business model. This is the approach taken in Oregon's, Connecticut's, and New Jersey's laws. These narrow definitions that broadly exempt businesses that have any kind of first-party relationship with a consumer are easier to administer from the business's perspective—determinations can be made on a per-customer basis and the rule is bright-line. It risks being underinclusive, however, particularly if a consumer's acceptance of terms of service or acknowledgement of a privacy notice could legitimize downstream data collection and sharing even if that data was collected in a different context (e.g., use of a tracking pixel on a distinct website).

A **broad** definition of data broker would be any business that sells personal data. To date, no state has enacted a definition this broad, although New Jersey's law applies to both data brokers and "data collectors," businesses that have a direct relationship with a consumer but who sell personal data to data brokers to register. If the purpose of the law is to broadly regulate the sale of data, then this approach could support that purpose by providing greater insight into the data brokerage ecosystem. However, if the purpose of data broker registration laws is to provide a consumer the ability to identify the businesses unknown to the consumer which are collecting the consumer's personal data, then this approach risks being overinclusive and overwhelming consumers with too many registered entities.

Several states, such as California, Texas, and Vermont, have opted for an **intermediate** definition. These states' definitions of data broker focus on the manner in which the data was collected—whether it was collected "directly" by the data broker or if it was collected outside the context of a first-party interaction.

[42] *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014). *But see* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. Rev. 1501 (2015).

This is a more flexible approach that centers consumer expectations and a consumer's intentional decision to interact with a business. That same flexibility makes this definition more difficult to operationalize.

Use Cases: Broad Regulation of "Data Brokerage" versus Targeted Prohibitions

Rather than a "one-size-fits-all" approach to data brokerage, policymakers may be interested in regulatory frameworks that focus on restricting certain harmful use cases while permitting other socially beneficial ones. One of the difficulties in this approach is that it requires stakeholder consensus about the harms and benefits different activities pose to individuals. Civil society organizations and privacy advocates may see some use cases, such as the sale of personal data to law enforcement or targeting consumers with advertisements based on sensitive data, as inherently **harmful or unduly risky**. Industry stakeholders may instead see some of these same use cases such as data sharing with law enforcement as **socially beneficial**. Industry and other stakeholders also identify other positive use cases (e.g., fraud prevention, anti-trafficking and anti-corruption law enforcement) that they believe are underrepresented in data broker policy conversations.

Participants in the FPF roundtable discussed three categories of harm: individual, government, and commercial. Participants expressed varying amounts of agreement on each of these categories. Stakeholders appeared most likely to conclude that **individual harms**—where one individual acting in their personal capacity uses brokered personal data to target another individual for stalking, harassment, violence, or another substantial injury—should be a priority in policy discussions. There was no argument that this conduct is beneficial and the injuries (e.g., physical, reputational, or financial) are readily apparent. Stakeholders appeared less likely to agree on the scope and severity of either benefits or harms from **government use** of brokered personal data. The starkest divide was on whether individuals experience tangible **commercial harms** from data broker activity. Direct marketing and targeted advertising, for example, may seem low risk or beneficial to some stakeholders while appearing as intrusive to others.

Identifying use cases to permit or proscribe requires meaningful insight into the data broker industry and understanding the activities (both harmful and beneficial) that would be disrupted by broad regulation of data brokerage. The term "data broker" could apply to numerous types of businesses, including those offering services related to: people-search websites; public-record aggregation; direct marketing, targeted advertising, and audience segmentation; data enrichment; location analytics; identity verification, fraud prevention, and risk management; background screening and eligibility-determination services; public-sector support, including law-enforcement; and more. A comprehensive overview of the data broker industry, including the different types of businesses and services that could fall under that label, could facilitate substantive, use-based regulations.[43]

[43] *E.g.*, Centre for Information Policy Leadership (CIPL), *Understanding Data Brokers: Definitions, Regulations, and Enforcement in the United States* (Discussion Draft April 2026), https://www.informationpolicycentre.com/wp-content/uploads/2026/04/CIPL_Understanding_Data_Brokers_Paper1_Apr26.pdf (providing examples of the types of services provided by data brokers, data collected, businesses' relationship to the information source, and data sources).

Safeguards: The Role of Existing Legal and Technical Protections

In developing any new state or federal data broker regulations, policymakers should consider the role that existing legal, technical, and self-regulatory safeguards play in addressing harms—where these safeguards work, where they show promise but leave gaps, and where they are no longer fit for purpose. **Existing legal safeguards**—including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Driver's Privacy Protection Act (DPPA), state comprehensive privacy laws, and prohibitions on unfair and deceptive trade practices—often regulate either the initial collection and disclosure of personal data or intended uses of that data. To the extent that policymakers are responding to harms stemming from conduct or data subject to one of these laws, one intermediate regulatory intervention could be increased funding for regulators to investigate violations, issue relevant guidance, and enforce these laws. Similarly, mapping how these laws apply to the different kinds of actors and services in the data broker ecosystem could identify gaps in protections that warrant targeted legislation.

Apart from statutory requirements, data brokers may also adopt voluntary standards or impose contractual obligations that proscribe certain uses of brokered personal data or restrict secondary uses of data altogether. Data brokers may also utilize **technical interventions**—such as the use of privacy enhancing technologies or data aggregation, deidentification, pseudonymization, or anonymization—that can mitigate the risk to consumers and facilitate socially beneficial data sharing. These **self-imposed measures**, sometimes known collectively as "data stewardship,"[44] can provide meaningful protections for consumers in the absence of law, although public awareness of them outside industry remains limited. At the same time, such voluntary measures are arguably most effective when accompanied by consistent oversight and enforcement. For example, Vermont's 2026 amendment to its law imposes due diligence requirements prior to disclosing brokered personal information. Policymakers could consider similar mandatory contractual and due diligence requirements, such as the CCPA's requirement that personal data can only be sold or shared with a third party subject to a contract that "[s]pecifies that the personal information is sold or disclosed by the business only for limited and specified purposes," amongst other requirements.[45]

Promoting Mutual Trust and Understanding to Support Evidence-Based Policymaking

One overarching theme that emerged from the roundtable is a lack of mutual trust and understanding between civil society, industry, and other stakeholders. Proponents and opponents of data broker regulation are rarely in direct communication and no one actor sees or represents the full picture of the data broker ecosystem. As a result, policymakers often receive conflicting information and inconsistent framing of key issues.

While the lack of direct interaction among stakeholders may not be unique to this particular policy area, it may be more acute due to the opaque nature of data brokerage. The individuals whose data is collected and sold by data brokers rarely interact with data brokers directly. Similarly, advocacy groups that support data broker regulation have noted consumers' "lack

[44] *E.g.*, Software and Information Industry Association (SIIA), "Data Stewardship," https://www.siia.net/data-stewardship-best-practices (last accessed July 20, 2026).
[45] Cal. Civ. Code § 1798.100, subd. (d).

awareness of how their data is collected, used, and disseminated."[46] Industry representatives, in contrast, have expressed frustration with regulatory proposals that they argue inadequately capture the nuance of businesses' data practices, omitting key details such as existing regulation, technical and legal safeguards in place, and responsible decisions about the purposes for which data is made available.[47]

In policy debates concerning privacy and data protection, the benefits of data collection and use (e.g., convenience) are often immediately recognizable whereas the harms to individuals are more abstract.[48] When it comes to data brokerage, that paradigm might be inverted. By lowering structural barriers to obtaining the information necessary to locate specific individuals, data brokerage can facilitate, enable, or amplify harms such as stalking, harassment, violence, or targeted manipulation.[49] These are individualized harms that present compelling narratives, particularly for policymakers and regulators tasked with protecting consumers from unfair or deceptive trade practices.[50] In contrast, potential benefits of data brokerage (e.g., fraud prevention in financial services, anti-trafficking, competition, risk management) are also more difficult to showcase because of the lack of direct relationship between a consumer and a data broker. This dynamic both undercuts the arguments about consumer choice that often predominate in privacy law and creates conditions for a lack of public trust. Left unaddressed, these features of the data broker ecosystem may continue to accelerate adoption of one-size-fits-all data broker regulatory frameworks.[51]

One step towards remedying that information asymmetry could be increased transparency from industry. The new wave of state data broker registration laws are attempting to bridge that gap by requiring detailed disclosures in the registration process. Policymakers want to understand what data is being collected, how it is being collected, what safeguards (administrative, legal, and technical) apply, to whom the data is being sold, and for what purpose the data is being sold.[52] Apart from legally mandated disclosures, industry actors can deepen trust by proactively

---

[46] Comments of EPIC, NCL, and CFA on the Protecting Americans from Harmful Data Broker Practices Notice of Proposed Rulemaking (April 2025), https://epic.org/documents/comments-of-epic-ncl-and-cfa-on-the-protecting-americans-from-harmful-data-broker-practices-notice-of-proposed-rulemaking.

[47] *See, e.g.*, Consumer Data Industry Association, Comment Re: Protection Americans from Harmful Data Broker Practices (Regulation V), (April 2025), https://www.cdiaonline.org/wp-content/uploads/2025/04/2025.04.02-Data-Broker-Comment-Letter-1.pdf (arguing that the proposed CFPB rule lacks sufficient data to support its policy conclusions and would disrupt activities such as law enforcement and antifraud efforts).

[48] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 816–819 (2022) (discussing the challenges of privacy harms, such as aggregation of small harms, future harms, and individual versus social harms).

[49] *Id.* at 832–33 (providing an example of a data broker being held liable for facilitating a third party's physical injury to another person).

[50] *E.g.*, Tom Uren, *Data Brokers Are a Killer's Best Friend*, LAWFARE (June 20, 2025), https://www.lawfaremedia.org/article/data-brokers-are-a-killer%27s-best-friend.

[51] Multiple states considered and enacted data broker legislation in 2026. Coyer, *supra* note 4.

[52] Memorandum, House Energy & Commerce Committee Staff, Re: Hearing on "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy," April 19, 2023, https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers ("[T]here are many unanswered questions about how this industry operates. Companies in this ecosystem often profit from selling Americans' personal data with little government oversight and in some cases, with minimal concern for or understanding of how the buyer intends to use the data. Meanwhile, Americans are often unaware of when data brokers have collected, purchased, sold, or shared their data. Because the disclosure of Americans personal data can lead to significant harms, data brokers must take stronger action to protect Americans' privacy.").

providing information about their data practices, as leading responsible actors in the space already do.

Conclusion

Regulatory interest in data brokers shows no signs of abating. In 2026 alone, at least sixteen U.S. states considered legislation that would have enacted or amended data broker registration laws.[53] Congress also considered multiple data broker bills, including as components of larger privacy and youth online safety packages.[54] It remains to be seen whether this burgeoning regulatory landscape will harmonize or diverge with respect to core definitions and obligations. If the trust deficit surrounding data brokerage continues to grow, it will only increase pressure for new regulation. Although stakeholders may disagree about the appropriate scope of regulation, there is a shared interest in reducing consumer harms while preserving responsible and beneficial uses of data. Doing so will require deeper dialogue between industry, civil society, and policymakers; greater transparency about existing industry practices and safeguards; and mapping of the data broker ecosystem. These steps offer a concrete, if challenging, path forward to increase trust, mitigate risks, and ensure delivery of socially beneficial services.

[53] HB 367, 2026 Reg. Sess., (Alaska 2026); SB 1790, 2026 Reg. Sess., (Ariz. 2026); SB 1104, 2025–26 Reg. Sess., (Cal. 2026); SB 4, 2026. Reg. Sess., (Conn. 2026) (signed May 27, 2026); HB 2463, 2026 Reg. Sess., (Haw. 2026);SB 3890, 2026 Reg. Sess., (Ill. 2026); SB 3219, 2026 Reg. Sess., (Ill. 2026); HB 4809, 2026 Reg. Sess., (Ill. 2026); SB 616, 2026 Reg. Sess., (Md. 2026); HB 1089, 2026 Reg. Sess., (Md. 2026); HF 4456, 2026 Reg. Sess., (Minn. 2026); HB 1694, 2026 Reg. Sess., (N.H. 2026); A5328, 2026–27 Reg. Sess., (N.J. 2026) (enacted June 30, 2026); SB 192, 2026 Reg. Sess., (N.M. 2026); S9131, 2025–26 Reg. Sess., (N.Y. 2026); A974, 2025–26 Reg. Sess., (N.Y. 2026); A9642, 2025–26 Reg. Sess., (N.Y. 2026) SB 2766, 2026 Reg. Sess., (R.I. 2026); HB 638, 2026. Reg. Sess., (Va. 2026); HB 2483, 2026 Reg. Sess., (Wash. 2026).

[54] Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, H.R. 8413, 119th Cong. (2026); Kids Internet and Digital Safety Act, H.R. 7757, 119th Cong. (2026) (engrossed June 29, 2026); H.R. 2612, 119th Cong. (2026); H.R. 4402, 119th Cong. (2025); H.R. 9482, 119th Cong. (2026); S.1287, 119th Cong. (2025); S.1512, 119th Cong. (2025); S.2144, 119th Cong. (2025); S.2850, 119th Cong. (2025); S.2851, 119th Cong. (2025).

Washington, DC | Brussels | Singapore

FPF.org