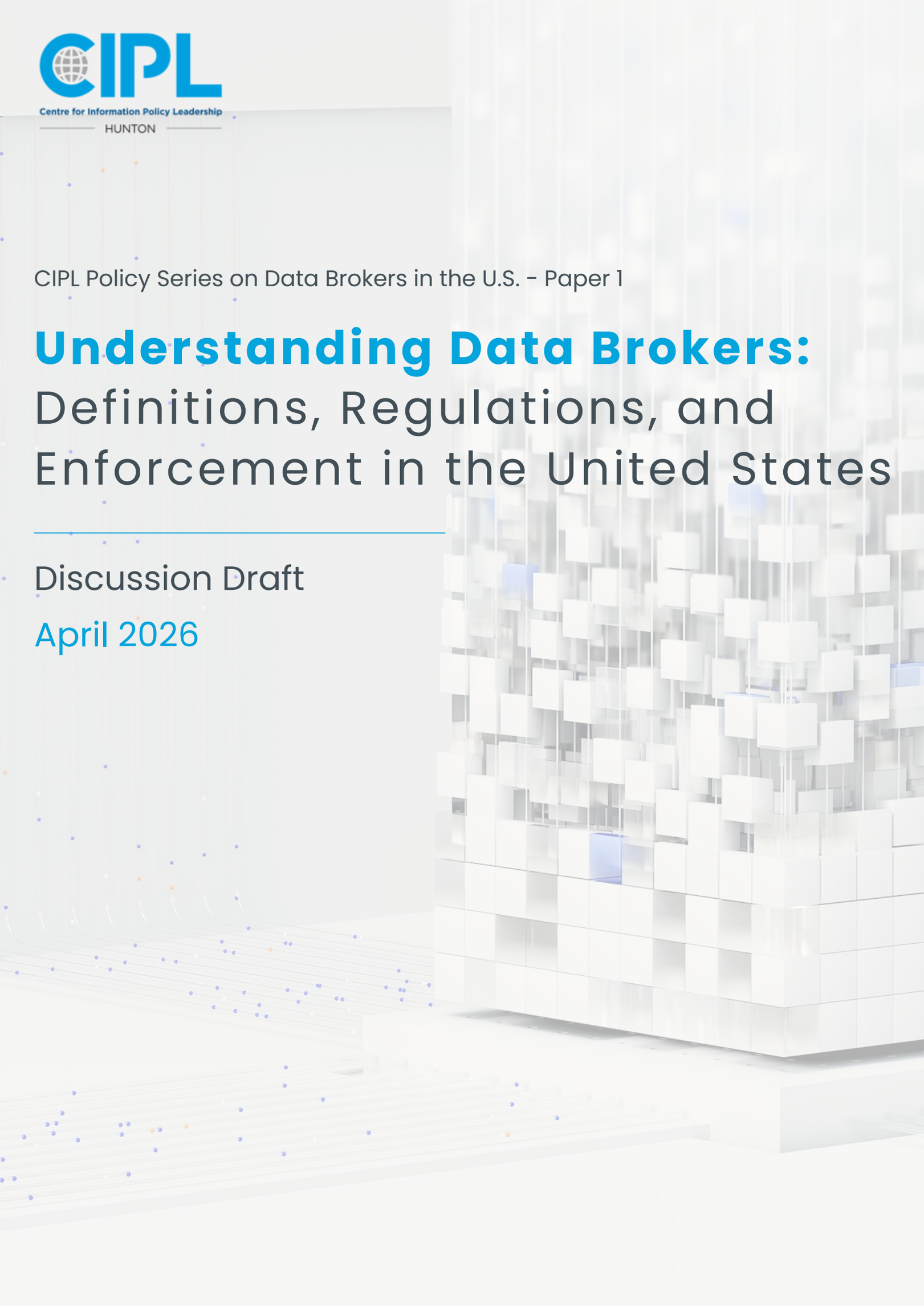
Centre for Information Policy Leadership
HUNTON

CIPL Policy Series on Data Brokers in the U.S. - Paper 1

Understanding Data Brokers: Definitions, Regulations, and Enforcement in the United States

Discussion Draft

April 2026



Understanding Data Brokers: Definitions, Regulations, and Enforcement in the United States

CIPL Policy Series on Data Brokers in the U.S. – Paper 1

Data is the foundation of the modern digital economy and society—fuel for innovation, business transformation, technological advancements, and services for consumers. At the heart of this dynamic marketplace are entities that gather data and make it available for beneficial uses, including the development of new products, services, and insights. The data collected includes both personal data (which is commonly defined as information that is linked or reasonably linkable to an identified or identifiable individual) and non-personal data.

With regard to the collection and use of individuals' personal data, there are a number of players in this space, but, for simplicity, they can be divided into three groups: first parties who have a direct relationship with the underlying individual, second parties who access data through a relationship with the first party, and third parties who gather information about individuals from other sources. These third parties are often labelled as "data brokers," but all three to some extent engage in the brokerage (i.e., the exchange or sale) of data.

The data broker industry operates at the intersection of commerce, privacy, and technology. Despite its ubiquity and impact, the industry remains poorly understood by policymakers, largely invisible to the individuals whose information fuels its operations, and disparately and insufficiently regulated by existing legal frameworks.

This three-part series examines the data broker landscape and proposes solutions that consider the breadth of the data broker industry, the benefits of proportionate, risk-based regulation, and the need for robust accountability mechanisms.

Paper 1 (this paper) establishes essential definitions and regulatory foundation.

We examine what data brokers are, how they operate, and how U.S. law currently defines and regulates them across federal and state laws.

Paper 2 explores the controversy and proportionality challenge.

We examine stakeholder perspectives and analyze the spectrum of data broker practices from clearly legitimate to problematic, arguing that effective regulation must differentiate among practices rather than treating all brokerage equally.

Paper 3 advances accountability and data stewardship as essential complements to regulation.

We examine governance frameworks and organizational practices that operationalize principled data handling, demonstrating that legislation and accountability are not alternatives but interdependent elements of effective privacy protection.

In sum, data broker policy requires multiple interventions working together, with each reinforcing the others to create comprehensive, adaptable, and enforceable data governance that is resilient and genuinely protective of individuals' rights in the digital age.

I. What are Data Brokers?

The data brokerage industry comprises a wide spectrum of businesses that collect and use both personal and non-personal data in different ways for a variety of purposes, products, and services. These businesses can be categorized or classified as data brokers by the services they provide, by the types of data they collect, by their relationship to sources of information, or by a combination of these elements:

Business Services Provided

- Consumer credit reporting
- Marketing data, analytics, and audience segmentation
- Data enrichment and enhancement
- Identity resolution and management
- Risk mitigation and fraud prevention
- Business credit information and due diligence
- Customer data platform and activation services
- Digital media and addressable advertising
- Locate and skip tracing services

Types of Data Collected (with increasing levels of sensitivity)

- Publicly available information (i.e., information generally available or accessible in the public domain without restriction)
- Business contact details and other business-to-business (B2B) information
- Public record information (a.k.a. "government record" information)[1]
- General demographics (such as census tract information, neighborhood-level socioeconomic characteristics, and other geographically aggregated statistical data)
- Individual and household demographics (e.g., age, gender, marital status, household composition, presence and ages of children, education, occupation, professional and employment history, estimated income, dwelling type, ethnicity, and language preference)
- Property, vehicle, and asset data (e.g., real property records showing dwelling type, purchase price, mortgage amount, home equity; vehicle ownership records showing make, model, year, registration)
- Lifestyle, interests, and attitudinal data (often self-reported and modeled on consumer preferences, hobbies, brand affinities, media consumption, psychographic profiles, and life event triggers (e.g., new parents, new movers, new homeowners))
- Industry-specific information (e.g., automotive in-market models and purchase intent; insurance behavioral segments; real estate and mortgage analytics; healthcare-related interest indicators)

- Shopping interests, imputed purchase categories and price ranges, history, online behavior, inferred interests, social media activities and charitable giving data
- Online behavioral and digital activity data (browsing behavior, online purchasing indicators, device and channel data, mobile app usage, and inferred digital interests)
- Financial behavior data (e.g., summarized credit statistics, creditworthiness indicators, investment activity, card usage, insurance tendencies, and financial distress indicators)
- Personal identifiers (e.g., driver's license number, social security number, and date of birth)
- Health information, precise geolocation, account login, citizenship data, minors' data
- Biometric and genetic information, reproductive health/abortion data, religious, union or political affiliations

Relationship to the Information Source

- *First Parties*. Direct relationship with consumers (first-party collector) with resale (i.e., brokerage) of that data (e.g., Epsilon's Shoppers Voice survey program; Acxiom's collection through warranty cards, product registrations, and contest entries)[2]
- *Second Parties*. No direct relationship with consumers, but relationship with first-party collector (e.g., Experian's ConsumerView, which compiles data furnished by creditors, lenders, and commercial partners; transactional data obtained by Acxiom and Epsilon from retailers and merchants)
- *Third Parties*. No direct relationship with consumers and no relationship with first-party collector (i.e., the compilation-of-compilations model, where a broker acquires data from other compilers or intermediaries)

Sources of Information

Data brokers can also be classified based on their underlying sources of information. In 2014, the U.S. Federal Trade Commission (FTC) identified several broad categories of sources from which data brokers collect data[3]:

- Federal government sources (e.g., demographic and statistical information from the U.S. Census Bureau; home address data (including change-of-address records) from the U.S. Postal Service)
- State and local government sources (e.g., county assessor and recorder property records; voter registration files; professional and occupational licenses; hunting and fishing licenses; motor vehicle records;[4] and vital records)
- Publicly available sources (e.g., telephone directories, social media sites)
- Commercial sources (including commercial compilers of the public records mentioned above; transactional data from retailers, merchants, and financial institutions; loyalty program data; magazine subscription lists; and product registration and warranty data, subject to regulatory constraints or restrictions)[5]
- Self-reported and survey sources (data provided directly by consumers through proprietary survey instruments, questionnaires, warranty cards, product registrations, and contest entries operated by data brokers or their partners)

Policy Takeaways

- Given the scope and breadth of these disparate elements, policymakers should assess whether data brokers are best defined by use case (i.e., services provided), by the type of data being brokered, and/or by the relationship to sources of information.
- Policymakers should take into account the range of business models, products, and services offered by the data broker industry, so as to ensure that proposed legislation and regulatory action are tailored to address only the business practices intended to be regulated.

II. U.S. Regulatory Landscape

While data brokers are sometimes characterized as being "unregulated," it is instead the case that the U.S. regulates data brokers through a patchwork of federal sectoral and state laws, in some cases creating gaps in consumer protection and creating complexity in compliance for industry. This fragmented landscape leaves consumers with inconsistent protections varying widely by geography and data broker type, while creating complexity and confusion for regulated entities. Unlike the European Union's (EU) comprehensive approach in the General Data Protection Regulation (GDPR),[6] U.S. federal data privacy regulations have incrementally evolved around specific sectors and harms, addressing data brokerage practices in isolated areas. Likewise, the state law landscape, especially so-called "comprehensive" privacy laws, can apply to data brokers in disjointed and disparate ways.

Federal Laws

In the absence of comprehensive federal legislation, all data collectors, including data brokers, are regulated under Section 5 of the Federal Trade Commission Act,[7] which empowers the Federal Trade Commission (FTC) to bring enforcement actions against them for inadequate security, deceptive marketing practices, or improper handling of sensitive data.

Data brokers are also regulated under the Fair Credit Reporting Act (FCRA),[8] which in part protects consumer privacy by protecting information collected by consumer reporting agencies, and the Gramm-Leach-Bliley Act (GLBA),[9] which governs information-sharing by financial institutions.[10] These laws are jointly enforced by the FTC and Consumer Financial Protection Bureau (CFPB), with the CFPB as the primary regulator. However, both the FCRA and the GLBA are limited to the consumer financial privacy context.

Data brokers are also subject to other sectoral laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its Privacy Rule, which protects individuals' medical records and other individually identifiable health information.[11] The related Security Rule protects electronic personal health information that is created, received, used, or maintained by a covered entity.[12] The Driver's Privacy Protection Act (DPPA)[13] applies to personal information assembled by State Departments of Motor Vehicles (DMVs), and the Family Educational Rights and Privacy Act (FERPA) applies to educational records.[14]

More recent federal laws and regulations address the impact of data brokers on national security. The Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA)[15] makes it unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to any foreign adversary country; or any entity that is controlled by a foreign adversary. Although a violation of the statute is treated as a violation of a rule defining an unfair or a deceptive act or practice under the FTC Act,[16] its focus on transfers of data to foreign adversaries is based on matters of national security.

Similarly, the Department of Justice's "Bulk Data Transfer Rule"[17] — which, among other things, prohibits or restricts certain data brokerage transactions that could result in access to bulk U.S. sensitive personal data by a "country of concern" — is intended to address the threat of foreign powers and state-sponsored threat actors using Americans' sensitive personal data for malicious purposes.

Given the very targeted focus of these federal laws and regulations, many data broker activities fall outside of these restrictions, creating gaps that states are motivated to address separately. This fragmented approach creates compliance challenges and inconsistency in terms of consumer rights.

State Regulation

States have increasingly focused on data brokers either in stand-alone laws or as a part of their comprehensive state privacy laws. As noted above, the comprehensive privacy laws arguably cover data brokers to the extent they fall within the definition of a controller, processor, or service provider.

Like many state comprehensive privacy laws, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), does not refer specifically to "data brokers," but it grants consumers certain rights regarding the collection, correction, transfer, and deletion of their personal information. Notably, California's law significantly impacts entities whose business practices involve the collection and sale of consumer data.[18] It also establishes an opt-out preference signal mechanism and requires businesses to honor browser-based privacy controls.

Data broker-specific laws, such as the one passed by Vermont in 2017, seek to foster transparency for consumers by establishing a public data broker registry. Vermont's law requires entities that "knowingly collect and sell or license to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship" to register with the state annually, pay fees, implement security programs, and provide breach notifications.[19] Texas[20] and Oregon[21] enacted similar registration laws in 2023.

California initially established a broker registry law in 2019,[22] and it subsequently amended that law with the Delete Act in 2023.[23] The Delete Act requires the California Privacy Protection Agency (CalPrivacy) to create a platform that allows consumers to request deletion of their personal information from all registered data brokers through a single request. CalPrivacy launched that platform—called the Delete Request and Opt-out Platform (DROP)[24]—in January 2026, with brokers required to process deletion requests through the DROP system starting August 1, 2026.

Perceived Regulatory Gaps

U.S. laws at both the state and federal level lack uniformity in the scope of their objectives with regard to data brokers. This results in a fragmented regulatory landscape that mandates different obligations and requirements across federal and state regimes. This patchwork is reflective of the differing priorities for legislative and regulatory intervention—some focus on consumer privacy, others on consumer transparency or consumer redress, and still others on national security concerns.

Policy Takeaways

- At the federal level, policymakers have addressed the data brokerage industry in many discrete, unrelated contexts, such as financial privacy, medical records, and national security.
- At the state level, policymakers have focused on data broker transparency, data security, and consumer privacy (specifically, opt-out) rights.

III. How Are Data Brokers Defined in U.S. Law?

The definition of the term "data broker" varies widely across the laws mentioned above, with significant implications for compliance and enforcement. Each statutory definition often hinges on the activity of data brokers through verbs—such as "collect," "sell," "license," or "share"—to differentiate between the types of activity triggering compliance obligations.

Some statutes, such as state comprehensive privacy laws, do not use or define the term "data broker," but they have broad definitions of "controller" that may include data brokers if they process personal data and meet the laws' thresholds.

As for statutes that specifically define the term "data broker," some focus on *third party sales of data* from entities that *do not have a direct relationship* with the individual whose data is being sold. For example, California and Vermont define the term "data broker" with reference to a business that sells (or licences) the personal information of a consumer with whom the consumer has no direct relationship.[25] These states notably also have a knowledge requirement for businesses falling within the definition, i.e., businesses that "knowingly" collect and sell the personal information of consumers to third parties.

In contrast, Texas does not have a knowledge requirement, but it defines a data broker as "[a] business entity that collects, processes, or transfers personal data that the business did not collect directly from the individual linked or linkable to the data."[26] There is no reference to a "direct relationship," but rather a reference to a direct collection.

Oregon's law does not differentiate between first-party and third-party collection.[27]

Some statutes may cover situations involving first-party collectors—i.e., businesses that have a direct relationship with a consumer—but who nonetheless engage in brokerage transactions. For example, under

the CCPA/CPRA, first-party collectors who sell personal information can have obligations similar to data brokers, even if they do not meet the definition of "data broker" under California's data broker registration law.

In a 2012 report,[28] the United States Federal Trade Commission (FTC) described data brokers as "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."[29] There is no reference to a direct relationship to (or direct collection from) a consumer whose data is resold. Nor is there a differentiation between a data broker that provides services to a company/client that has a direct relationship with the consumer and a data broker that provides services to a company that lacks any relationship with the consumer.

Aside from the relationship factor, the definitions of "personal data" covered by these laws differ among the states, with Texas, for example, exempting deidentified data, employee data, and publicly available information.[30] California notably includes employment-related information within its definition of personal information.[31]

Under U.S. federal law, the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA) defines "data broker" 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."[32] Notably, this definition is not limited to "personal data."

The U.S. Department of Justice's "Bulk Data Transfer Rule"[33] defines the term "data brokerage" as "the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."[34] Notably, this definition, too, is not limited to "personal data." The Rule prohibits "covered data transactions involving data brokerage with a country of concern,"[35] and "covered data transactions"[36] include the brokerage of "government-related data,"[37] which is not limited to personal information.

The lack of uniformity in these definitions and in the scope of coverage creates operational complexity for data broker organizations. This heterogenous regulatory environment not only complicates enforcement, but also increases the risk of conflicting obligations

Policy Takeaways

- Policymakers should tailor the definition of "data broker" to the business model(s) or business practice(s) they are seeking to regulate.
- Policymakers should consider whether the lack of a "direct relationship" with the underlying consumer, in and of itself, should be the sole criterion for triggering obligations, or whether obligations should depend on the purposes for which the personal information will be used.

- Policymakers should differentiate between different types of business models, products, and services by considering the underlying purpose(s) and objective(s) of a broker's activities. For example, policymakers should ensure that business models offering risk mitigation, identity verification, fraud prevention, due diligence, and other B2B services do not inadvertently fall within the scope of a statute that purports to regulate consumer marketing practices, for example.
- Policymakers should assess whether the brokerage of non-personal information should fall within the scope of a given law.
- Policymakers should assess whether personal information collected from certain sources (such as public records) should fall within the scope of a given law, as well as the consequences (both intended and unintended) of any compliance obligations.
- Policymakers should consider the type of relationship that a data broker's client has with the consumer and the type of services provided by the data broker for the client.

REFERENCES

1. Generally available under FOIA laws, with mitigating statutes that restrict and regulate specific types of data from government sources. Examples include driver's license data available for 14 permissible uses under the federal Drivers Privacy Protection Act (DPPA) and analogous state laws; real property assessor and recorder records used for real estate, financial, and insurance applications and regulated by state law; voter registration files, regulated by state law for specific purposes only; and professional and occupational licenses.

2. First party collectors could also encompass large digital platforms that collect real-time behavioral data points from direct interactions with their users and then use that data to power advertising, content recommendation, and product development.

3. Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014), available at https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

4. Subject to restrictions by the Drivers Privacy Protection Act, 18 U.S.C. § 2721, et seq.

5. Commercial sources can include businesses such as retailers, social media companies, and financial service companies, who share their customer data. Yuhui Lin, *Derived Information Provided by Data Brokers for Marketing Purposes: An Elaborate Consumer Profile*, 34 CORNELL J. L. & PUB. POL'y 133 (Fall 2024).

6. Regulation (EU) 2016/679, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

7. 15 U.S.C. § 45.

8. 15 U.S.C. § 1681 et seq.

9. Codified in relevant part primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827.

10. 15 U.S.C. § 6801.

11. See https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

12. See https://www.hhs.gov/hipaa/for-professionals/security/index.html.

13. 18 U.S.C. § 2721.

14. 29 U.S.C § 1181, 18 U.S.C. § 2721, and 20 U.S.C. § 1232g.

15. 15 U.S.C. § 9901 et seq.

16. 15 U.S.C. § 9901(b)(1).

17. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 FR 1636 (Jan. 8, 2025).

18. *Id*; *see also* Cal. Civ. Code §§ 1798.105, 1798.135 (2023).

19. 9 V.S.A. § 2430(1)(A).

20. Tex. Bus. & Com. Code § 510.001 et seq.

21. Or. Rev. Stat. § 646A.593.

22. California Session Laws, Stats. 2019, ch. 753, codified at Cal. Civ. Code § 1798.99.80 et seq.

23. California Session Laws, Stats. 2023, ch. 709.

24. See https://privacy.ca.gov/drop/.

25. Cal. Civ. Code §1798.99.80(c); 9 Vt. Stat. §2430(4).

26. Tex. Bus. & Com. Code § 510.001.

27. "'Data broker' means a business entity or part of a business entity that collects and sells or licenses brokered personal data to another person." Or. Rev. Stat. § 646A.593(1)(c)(A).

28. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

29. In its 2012 report, the Federal Trade Commission (FTC) described three different categories of data brokers (1) entities subject to the Fair Credit Reporting Act (FCRA) ; (2) entities that maintain data for marketing purposes; (3) non-FCRA covered entities that maintain data for non-marketing purposes that fall outside the scope of FCRA.

30. Tex. Bus. & Com. Code § 510.001 (11).

31. Cal. Civ. Code § 1798.140(v)(1)(I).

32. 15 U.S.C. § 9901(c)(3)(A).

33. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 FR 1636 (Jan. 8, 2025).

34. 28 C.F.R. §202.214(a).

35. 28 C.F.R. §202.301(a).

36. 28 C.F.R. §202.210(a)(1).

37. 28 C.F.R. §202.222.

Who We Are

The **Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.