CIPL Centre for Information Policy Leadership
HUNTON

CIPL Policy Series on Data Brokers in the U.S. - Paper 2

Data Brokers and Proportionate Regulation: Balancing Commercial Value, Consumer Protection and Civil Rights

Discussion Draft

May 2026

Data Brokers and Proportionate Regulation: Balancing Commercial Value, Consumer Protection, and Civil Rights

CIPL Policy Series on Data Brokers in the U.S. – Paper 2

The data broker industry defies simplistic characterization. It encompasses a spectrum of businesses, both legitimate and problematic. It includes entities stopping fraud, as well as those enabling stalking; companies expanding credit access for underserved populations, and those targeting seniors with predatory offers; aggregators enabling life-saving medical research, and those selling sensitive location data. This complexity demands regulatory approaches that differentiate among practices and use cases. Policymakers should refrain from imposing uniform restrictions that eliminate beneficial activities and from creating categorical bans that drive harmful practices underground. Treating data brokers identically through blanket regulation risks eliminating benefits without adequately addressing harms.

This paper is the second in a three-part series examining data brokers in the United States.

Paper 1 establishes foundational elements: defining data brokers, examining current laws that regulate their practices, and highlighting the fragmented legal landscape.

Paper 2 (this paper) addresses the proportionality challenge: fostering regulation that protects consumers from documented harms while preserving legitimate commercial activities and avoiding unintended consequences.

Paper 3 advances accountability and data stewardship: examining governance frameworks and organizational practices that operationalize principled data handling.

I. Why Have Data Brokers Attracted Attention from U.S. Policymakers?

Data brokers have increasingly become the focus of legislative and regulatory attention because of their collection and use of personal information about individuals—largely without the knowledge of those individuals—that may impact personal privacy, cybersecurity risks, civil rights, business operations, national security, and other important concerns.

Privacy

Data brokers collect and sell the personal information of individuals with whom they usually have no direct relationship. This makes traditional notice-and-consent frameworks and perceived protections that they afford to individuals functionally impossible to implement. While CIPL has recognized that the notice-and-consent model has significant limitations when it comes to realizing consumer protections and governing

the processing of information in a digital society,[1] it nevertheless plays a role in many processing activities. In such instances, consumers may be unaware of the information brokers have about them and would be unable to request the correction of inaccurate information, prevent harmful uses, or otherwise exercise their rights with respect to that information.

The industry's perceived obscurity—operating "behind the scenes" as the FTC characterized it[2]—may itself be enough to pique regulatory interest. But when news accounts detail data brokers' involvement in data breaches,[3] discriminatory targeting of vulnerable populations,[4] stalking or doxxing of individuals,[5] and government surveillance without warrants,[6] bipartisan interests coalesce to address these distinctive harms, principally in the context of consumer privacy laws. While data brokers' products and services can and do provide substantial benefits to individuals, organizations, society, and the economy in many contexts, these are sometimes not considered or well understood. Finally, significant risks associated with some players within the industry—such as those identified above—have justifiably warranted legislative and regulatory scrutiny.

Transparency and Control

Many consumers are unaware of the data brokerage industry, the information that is collected about them, how the data is used, or the entities to whom their data is sold or licensed. They may also be unaware of their rights, such as correction and opt-out rights, which exist under some U.S. state laws. To the extent some data brokers may offer explanatory materials and opt-out mechanisms, consumers may find such materials to be confusing or difficult to navigate. These limitations make it difficult for consumers to exercise control over their personal information and make well-informed choices.

National Security

Unless guardrails are in place, data brokers can create vulnerabilities by enabling hostile foreign actors to acquire broad and large volumes of personal information on U.S. citizens. This data can include sensitive information such as geolocation histories, purchasing behaviors, health-related information, and financial patterns, which, when aggregated, can yield highly sensitive insights into the habits, affiliations, and vulnerabilities of individuals in key positions, such as government officials, military personnel, and workers responsible for critical infrastructure. When this information is available through commercial transactions, it may not be subject to the same vetting requirements as those required by defense contractors or intelligence agencies. Moreover, foreign adversaries can exploit this information to conduct cyberattacks, blackmail, and disinformation campaigns. They can also influence government operations and democratic processes by targeting specific individuals or groups, including in the context of elections and political campaigns.[7] The Protecting Americans' Data from Foreign Adversaries Act (PADFAA)[8] and the U.S. Department of Justice's "Bulk Data Transfer Rule"[9] were enacted to address these risks.

Civil Rights

When aggregating and analyzing large quantities of personal information, data brokers can create consumer profiles that include race, ethnicity, income, gender, and other data deemed sensitive. While some of the uses are benign or actively intended for use to combat discrimination (e.g., in AI model training), their use in other circumstances could exacerbate biases or enable unlawful discrimination. It should be noted, however, that such abuses are not representative of all members of the data brokerage industry.

Fraud

While some categories of data brokers can and do help financial institutions, companies, and law enforcement verify identities, detect financial anomalies, and flag other potentially fraudulent activities, the same data—in the wake of a breach or other security incident—can be used by criminal actors to commit identity theft, misappropriation, and fraud. The commodification of personal information is a thriving underground market where stolen or leaked data is combined with legitimate, broker-sourced data to enhance its utility for criminal purposes. Admittedly, however, this risk is not limited to the data broker industry.

Cybersecurity

The concentration of vast amounts of personal data within the data broker ecosystem creates cybersecurity responsibilities that leading companies in the industry take seriously. Data brokers compile and store information from diverse sources, and responsible actors implement stringent security controls and breach notification protocols commensurate with the sensitivity and scale of the data they steward. However, actors that fail to maintain adequate security standards create vulnerabilities that attract cybercriminals and expose downstream systems to supply chain risk. Inadequate security measures—such as outdated encryption protocols, insufficient access controls, or failure to segment sensitive datasets—further exacerbate the threats. A single breach of a large data broker business can expose hundreds of millions of individual records with cascading effects across multiple industries. This makes adoption of best-in-class cybersecurity protections and governance essential for responsible actors in the industry.

Policy Takeaway

- Policymakers should carefully consider the severity of documented harms from some data broker practices, which can affect consumer privacy, civil rights, business operations, national security, and other important concerns.

II. Legitimate Purposes and Societal Benefits

When used responsibly, data brokers' datasets and services enable substantial benefits for the economy and society, such as detecting and preventing cybercrime, recognizing and facilitating trusted transactions, documenting consumer behaviors relevant to health research, and informing critical business and policy decision-making. To enable these benefits, data brokers analyze large and diverse amounts of data from various sources to identify connections and patterns related to identities and businesses. Understanding these benefits can help lawmakers create policies that protect individuals while preserving the economic and societal values generated through responsible data use and sharing.

We identify below key beneficial data uses, services, and products commonly offered by data brokers.

Customer Experience and Personalization

From tailored products to personalized experiences, data brokers enable companies to deliver relevant, efficient, and user-friendly services. Customers benefit when data is used to improve services that align with their needs and preferences.

Case Study

- ***Customer Relationship Management –*** *Digital marketing is critically important for small and medium-sized businesses, which comprise the majority of American businesses. Data brokers offer solutions that identify connections between customers and vendors to optimize marketing efforts. This technology individualizes services to help businesses strengthen customer relationships and improve customer acquisition and retention rates.*

Identity Verification and Authentication

Data brokers leverage data across industries to enable a system of identity validation and authentication that is essential to removing obstacles for legitimate customers and detecting anomalous behavior. By providing identity verification, data brokers help expose financial crimes like money laundering and fraud, ensure stability of financial systems, help companies comply with financial regulations, and protect consumers from harm. Without these services, businesses would violate compliance obligations and face fines, suffer reputational damage, and incur operational disruption; consumers could face financial ruin. Moreover, the increased need for identity verification and authentication in the digital ecosystem and infrastructure are likely going to expand use cases and the need for data brokerage services across various sectors.

Case Study

- ***Know Your Customer Software –*** *A data broker offers a service that analyzes digital and physical data points to verify and confirm a person's identity quickly through a multi-layered*

authentication approach. This product works efficiently to differentiate trusted customers from high-risk ones in a way that prevents fraud while ensuring a high-quality customer experience.

Fraud Detection and Prevention

Data brokers use complex data sets to support financial investigations, combat fraud, prevent improper payments, and recapture lost revenue. By providing fraud detection services, data brokers help organizations prevent incidences of identity theft, deter fraudulent transactions, and comply with regulatory obligations.

Case Study

- ***Behavioral Intelligence*** *– Providers use behavioral intelligence to scan certain online behaviors—such as typing keystrokes—to assess the likelihood of legitimate versus fraudulent activity based on a user's previous behavior. Businesses can use these services to identify threats to legitimate users and provide comprehensive fraud protection for consumers.*

Compliance and Due Diligence

Businesses of all sizes have the challenge of navigating an ever-changing regulatory landscape. The services provided by data brokers can help a business understand and navigate changing regulations by streamlining due diligence workflows to reduce financial exposure and reputational risks.

Case Studies

- ***Automating Due Diligence Processes –*** *Providers offer technologies that organizations can use to automate and standardize elements of risk assessment. Organizations using such services are able to apply a consistent risk-based approach when evaluating financial parties to ensure that decisions are evidence-driven and well documented.*
- ***Increasing Accuracy in Due Diligence Processes*** *– Data brokers offer solutions that verify, for example, whether a consumer owns the property for which the consumer is seeking to use as collateral for a loan, or about which the consumer is seeking to apply for disaster aid relief.*

Risk Mitigation

Data brokers play a central role in risk mitigation across financial services, insurance, and security-related industries. Companies in these industries use data brokers' services to identify the financial and regulatory requirements and assess and mitigate risk associated with their business operations.

Case Study

- ***Account Monitoring –*** *Data brokers offer services that support organizations' efforts to establish financial crime compliance programs in industries such as retail and technology. The services include ongoing monitoring, customer and vendor risk assessment, and sanctions and watchlist screening, allowing a business to efficiently recognize relevant risks and complete critical financial crime compliance processes across the lifecycle of the customer.*

Data Management and Quality:

Data brokers can analyze data and deliver actionable insights. Businesses can then leverage those insights to improve the accuracy of their data, reveal new business opportunities, and improve performance.

Case Study

- ***Insights for the Health Industry –*** *A data broker offers health information on the U.S. adult population that includes social determinants of health, medical claim information, and mortality. The broker uses de-identification tools to create datasets for healthcare providers and clinical researchers to aid them in their research and improve outreach to at-risk patients.*

Policy Takeaway

- Policymakers must recognize that data brokers provide significant beneficial and legitimate services to combat fraud, prevent identity theft, enable due diligence, mitigate risk, and facilitate regulatory compliance.

III. Proportionate Regulation: A Risk-based Framework

Data brokers operate within a complex ecosystem where many activities serve genuine societal, commercial, and individual benefits. At the same time, there exist underlying risks and potential harms from their practices. Finding a proportionate, risk-based approach to regulation, oversight, and compliance is essential to address potential harms while enabling beneficial practices. Understanding legitimate use cases is a vital first step for crafting proportionate regulation and a nuanced policy framework.

A related principle must also be understood: data itself is neither beneficial nor harmful—it is the application and use of data that determines whether the resulting impact is beneficial or harmful to individuals, to society, and to the economy. The same dataset that enables a bank to extend credit to an underserved borrower could, if misused, enable discriminatory denial of services. The same consumer profile that helps a retailer stock the right products on the right shelves could, in the wrong hands, be used for predatory targeting. This principle has profound implications for regulation: effective policy must focus on the use of data and the resulting consequences, not simply on the collection or existence of data.

For each category of data use outlined in this paper, there are different magnitudes of potential benefit and different magnitudes of potential harm—and, critically, different solutions to mitigate those harms while preserving those benefits. A proportionate regulatory framework must account for this graduated spectrum rather than treating all data uses as presenting equivalent risk.

CIPL recommends the adoption of a risk-based framework that would require data brokers to justify their processing activities through documented assessments. These assessments would recognize that data broker activities exist on a spectrum from clearly beneficial (such as fraud prevention) to potentially harmful (including predatory marketing and discriminatory profiling). CIPL recommends policymakers and industry to engage in conversations to help identify factors to consider when making such assessments.

Proportionality coupled with a risk-based approach would ensure (i) minimal restrictions on high-value, low-risk activities; (ii) enhanced oversight for sensitive data and vulnerable populations; and (iii) categorical prohibitions on practices lacking a legitimate purpose. This calibrated approach would enable beneficial data uses while constraining exploitative practices through documented justification requirements and regulatory accountability.

Finally, while U.S. privacy law has traditionally relied on a notice-and-consent model, application of that model to brokers' legitimate data collection and sharing activities could undermine the very essence and the purpose of some data uses. For example, in the cases of fraud prevention, financial regulations, or export and sanctions controls, seeking consent would either be irrational or undermine the purpose of processing. In such cases, compliance with a legal obligation or the existence of a reasonable basis would be the right concept to legitimize data collection, use, and sharing.

Policy Takeaway

- A proportionate, risk-based regulatory framework can promote beneficial broker practices while constraining harmful ones.

REFERENCES

1. CIPL Response to the U.S. House Committee on Energy & Commerce Privacy Working Group Request for Information, April 7, 2025, available at https://www.informationpolicycentre.com/resources/cipl-response-to-house-committee-on-energy-commerce-data-privacy-working-group-rfi-concerning-potential-us-federal-privacy-law/.

2. "Data Brokers: A Call for Transparency and Accountability," Statement of Commissioner Julie Brill, Federal Trade Commission (May 27, 2014), available at https://www.ftc.gov/system/files/documents/public_statements/311551/140527databrokerrptbrillstmt.pdf.

3. Donna LeValley, *Nearly 3 Billion People Hacked in National Public Data Breach. What You Need to Know*, https://www.kiplinger.com/personal-finance/billions-hacked-in-national-public-data-breach.

4. Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices—Right Now*, https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/.

5. Niamh Ancell, *Data brokers are constantly doxing us, and we can't do anything about it*, https://cybernews.com/security/data-brokers-doxing-interview/.

6. Aaron X. Sobel, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, https://yalelawandpolicy.org/end-running-warrants-purchasing-data-under-fourth-amendment-and-state-action-problem.

7. Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S. Military Personnel 15 (Nov. 2023), available at https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokersand-the-Sale-of-Data-on-US-Military-Personnel.pdf.

8. 15 U.S.C. § 9901 et seq.

9. 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).

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.