Centre for Information Policy Leadership
HUNTON

CIPL Policy Series on Data Brokers in the U.S. - Paper 3

Data Stewardship and Accountability: Operationalizing Responsible Data Broker Practices

Discussion Draft

May 2026

Data Stewardship and Accountability: Operationalizing Responsible Data Broker Practices

CIPL Policy Series on Data Brokers in the U.S. – Paper 3

Laws and regulations establish what organizations must do. Accountability gives them the means to do it. This distinction—between legal obligation and operational reality—represents the critical gap in privacy protection that prescriptive rules alone cannot bridge. Even the most comprehensive regulatory framework requires mechanisms that translate abstract principles into daily practices, permit flexibility for technological innovations, address context-specific challenges, and enable verification for effective implementation. This paper addresses how data brokers can operationalize regulatory obligations through data stewardship, accountability structures, and governance practices.

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

Paper 1 establishes the baseline: defining data brokers, documenting the fragmented U.S. regulatory landscape, and identifying potential gaps.

Paper 2 proposes a proportionate regulatory solution: acknowledging the spectrum of data broker activities from beneficial to harmful, examining stakeholder perspectives, and suggesting a risk-based framework with documented assessments. As those papers explained, policy reforms are necessary to address recognized harms and promote legitimate societal, commercial, and individual benefits.

Paper 3 (this paper) examines data stewardship and accountability as essential components to the regulatory framework. Effective data broker reform requires multiple layers working in concert: principled legislation, proportionate regulation, and robust accountability mechanisms—each building upon and reinforcing the other.

I. The Path Forward: Data Stewardship

The term "data stewardship" encompasses the ethical management and use of data, emphasizing the responsibility of data brokers to protect the privacy and security of consumers' data while fostering trust in their services. By examining best practices in stewardship, we can identify pathways for ensuring that the data brokerage industry delivers benefits to individuals, organizations, and society with responsibility and accountability.

A. Organizational Accountability

A fundamental concern about the data broker industry is a perceived lack of understanding and accountability. This concern has been an impetus for legislative proposals to create data broker registries, licensing requirements, and new consumer rights. However, it is important to recognize that many leading companies in the data broker industry have invested substantially in responsible data management, privacy governance, and accountability programs—in many cases well ahead of legal requirements. The challenge is that, in the absence of a more specific accountability framework, the regulatory environment has not adequately recognized or rewarded these companies. For those companies who have implemented robust controls, the ability to demonstrate accountability against a recognized standard is essential.

CIPL recommends the adoption of specific policy and regulatory measures, incentives, and approaches that encourage and promote demonstrable organizational accountability practices that ensure the responsible use and sharing of data.

While some organizations in the industry have invested heavily in responsible data management programs and practices, the lack of trust in the data broker industry as a whole has not benefited those organizations who have been leaders in accountability. Indeed, the broad-brush approach to most legislative and regulatory measures has failed to incentivize or identify what responsible data practices look like in practice. Hence, the race-to-the-top market mechanism that rewards best practices has not materialized within the industry as a whole, while those businesses who are true leaders, investing heavily in responsible privacy and security practices, are not recognized for their efforts.

To bridge this regulatory gap, data brokers should proactively embrace organizational accountability principles that go beyond the minimal compliance standards set by current law—as the most responsible actors in the industry are already doing.

CIPL has long advocated for organizational accountability as the best way to ensure responsible and effective data governance that enables beneficial innovation in tandem with the protection of individuals' personal data. Organizational accountability requires organizations to operationalize data privacy, security, and governance obligations with concrete controls, policies, procedures, tools, and actions. It also requires organizations to demonstrate the existence and effectiveness of their accountability measures, both internally to the board and senior management, and externally to regulators, individuals, business partners, and shareholders.

Accountability is not self-regulation; it is a framework that translates principles-based legal rules into concrete policies, procedures, controls, and governance to deliver compliance.

The seven elements of CIPL's Accountability Framework—Leadership and Oversight, Risk Assessment, Policies and Procedures, Transparency, Training and Awareness, Monitoring and Verification, Response and Enforcement—are designed to ensure a holistic approach to organizational practices and compliance measures. The framework assesses whether an organization's practices are sufficiently comprehensive and whether new governance programs should be developed. Adopting a framework for accountability is not simply about avoiding liability; it is about signalling a commitment to responsible data stewardship.

Source: CIPL

Case Studies

- ***Public Articulation of AI and Data Use Principles –*** *A leading data broker publishes a set of "AI and Data Use Principles" that apply across jurisdictions, irrespective of legal requirements. The principles include a commitment to explainability, meaningful human oversight, protection for privacy, and ensuring data is not used to create or reinforce unfair bias.*
- ***Acxiom –*** *In 1991, Acxiom became the first company on record to officially establish the role of Chief Privacy Officer, committing to Fair Information Practices with applied data ethics and operational data governance—more than a decade before most organizations considered privacy as a governance function. Acxiom has maintained a full range of privacy rights for individuals since that time. In 2004, Acxiom implemented an "ethical data sourcing" program to protect the reputation of both the company and its clients who rely on ethically sourced data.*
- ***Self-Regulation –*** *The data broker industry has established industry coalitions and collaborative governance bodies to develop codes of conduct, best practice standards, and accountability frameworks to help shape responsible data practices. These include the Information Accountability Foundation, the Coalition for Sensible Public Records Access, the Direct Marketing Association's data governance rules, the Online Privacy Alliance, the Individual Reference Services Group, the Digital Advertising Alliance, the Network Advertising Initiative, and the Email Sender & Provider Coalition.*

B. Meaningful Transparency

In the data broker context, many stakeholders have expressed a desire for more meaningful transparency in how consumers' personal data is collected, used, shared, and secured. To address this concern, data brokers should commit to transparency as a core operational principle. Transparency is more than an exercise of checking boxes, however. It demands a well-coordinated effort to clarify complex data practices for consumers.

To that end, data brokers should be held to standards that apply to first party collectors and implement tools that allow individuals to understand what information about them is being held and the purposes for which it is used and shared. This could include novel and innovative transparency mechanisms, such as dashboards, interactive privacy notices, as well as broader transparency and digital literacy campaigns about data use, AI use, and the role of brokers in the data ecosystem. Transparency measures could also enable the consistent facilitation of consumer rights, such as the right of correction or right of access present in many state comprehensive privacy laws. Meaningful transparency can often be combined with notice and other consumer rights practices. Importantly, proactive transparency should be viewed as a competitive differentiator. Organizations that proactively illuminate their practices can strengthen public trust, reduce the likelihood of enforcement actions, and position themselves as leaders in responsible stewardship of data.

Case Study

- ***Transparency Reports across Jurisdictions –*** *A leading U.S. data broker enables any individual in the United States to request and receive a report describing the data that the organization holds about them, regardless of whether the state in which they reside has adopted such requirements.*

C. Consumer Empowerment

One of the most persistent criticisms of the data broker industry is that their business model does not allow individuals to exercise sufficient control over their personal information. Unlike traditional B2C relationships, the relationship between a consumer and a data broker is indirect and often unknown to the consumer. The perceived absence of meaningful consumer choice has motivated some legislative efforts to impose strict opt-out obligations, for example.

To address this problem, data brokers should consider building clear, harmonized, and user-friendly consumer choice mechanisms into their operations, where feasible. These tools should be consistent across platforms, easily located, and able to be used without unnecessary barriers.

At the same time, there may be use cases where consumer choice mechanisms are neither optimal nor appropriate, such as in cases to prevent fraud or cyber risk, or to enable financial or export controls compliance. Nevertheless, by empowering consumers with meaningful choices where appropriate and by

adopting organizational accountability practices more broadly, data brokers can secure consumers' (and regulators') trust while ensuring the sustainability of the industry's data-driven business model.

It is important to note that consumer empowerment can be achieved above and beyond consent. CIPL has written about the limitations of consent as a basis for processing, given the challenges of scaling consent and the high burden it places on individuals.[1] Principles of transparency, redressability, fairness, risk assessment, and other elements of organizational accountability are actually more effective means to enable true consumer empowerment and the mitigation of potential harms.[2]

D. Appropriate Data Minimization

Data brokers are often criticized for collecting and retaining personal information without clear limitations or for using that information in ways that do not correspond to the original purposes of collection. To address these concerns, data brokers should consider adopting a disciplined approach to the data minimization principle.

Data minimization requires organizations to limit the collection of personal data to what is *adequate, relevant, and reasonably necessary* in relation to the purposes for which such data is processed, as disclosed.[3] It is closely related to the principles of proportionality, necessity, purpose limitation, collection limitation, and storage limitation.

CIPL has written about the importance of interpreting the data minimization principle thoughtfully, especially in the age of AI. The principle should not be viewed as an absolute limitation on the collection of large volumes of data, but should be interpreted so as to enable legitimate purposes, such as bias mitigation in model training.[4]

Data brokers can likewise apply the data minimization principle appropriately by sharing transparently the types of data collected and the purposes for collection, describing publicly the scope of their collection activities, and applying technical solutions and strategic design choices to minimize risks associated with the collection and use of personal data, such as through the use of privacy-enhancing technologies (PETs).

PETs are a critical component of every accountable data management system. They enable organizations to use and share data by mitigating privacy risks and enabling compliance with regulatory obligations. Their utility and importance will necessarily rise with the increased adoption of AI technologies and systems that rely on large volumes of data.[5]

Appropriately applied, data minimization can create a competitive advantage for data brokers by reducing their exposure to risks, while increasing consumer trust and addressing public concerns.

E. Internal Controls and Cybersecurity

Effective data stewardship requires data brokers to put in place robust controls to secure consumer data once it is collected. Many data brokers collect large data sets from diverse sources, creating central

repositories of sensitive personal information that become attractive targets for external attackers and vulnerable inventories for internal misuse. Lax or absent internal access controls increase the risk that an employee, contractor, or business customer may access data without the proper authorization and use it for purposes beyond what was originally intended.

To address these risks, responsible data brokers must adopt policies to ensure that data access and use are appropriately limited, monitored, and audited. The first step is ensuring that employees, contractors, and other business partners are able to access only the data necessary for their job functions. Data brokers should also establish logging and monitoring systems that track who accesses data, when, and for what purpose. These policies deter misconduct and reduce the likelihood of internal misuse and accidental disclosures.

To mitigate external cybersecurity risks, data brokers should implement data security safeguards including encryption access controls, incident response protocols, and continuous monitoring. If a serious breach occurs, data brokers should have processes in place to report the breach to the appropriate regulators. Strong internal controls and security practices serve as a safeguard for consumers and brokers alike.

Case Study

- ***Setting the Tone from the Top –*** *An organization has established a team of regional privacy lawyers and privacy officers who report to the CPO. They identify legal and regulatory requirements applicable to each region. These recommendations are reviewed against the organization's global privacy program to determine whether and to what extent local variations should apply across the globe, thereby leveraging global controls as much as possible.*[6] *Product development and data infrastructure teams engage proactively with these teams to ensure that "privacy by design" principles are embedded from the start.*

F. Due Diligence in Vetting Clients

Another key component of data stewardship is the vetting and verification of data brokers' clients—i.e., the third-party recipients of consumers' personal data—before granting them access to that data. Absent robust due diligence in vetting third-party recipients to ensure they are legitimate and capable of handling data responsibly, bad actors can obtain consumer data and significantly expose that data to harmful uses. Insufficient vetting can undermine a data brokers' entire data governance framework.

To address this weakness, data brokers must embed strong due diligence practices into their operations. At a minimum, data brokers should assess prospective clients' legitimacy before granting access to their data. Brokers should verify the corporate identity of prospective clients through official business registries, licensing databases, and independent third-party verification tools. Vetting should also examine ownership in order to prevent shell companies from successfully accessing data. It should also require documentation showing the recipient's need and purpose for acquiring and processing consumer data. Ensuring that

clients are legitimate, financially stable, and reputable businesses can reduce the risk of data misuse and reputation harm for data brokers.

Case Study

- ***Customer Credentialing and Ongoing Oversight –*** *Leading information services companies conduct rigorous client credentialing before granting access to consumer data. These practices can include verification of corporate identity and beneficial ownership, assessment of the client's intended use and permissible purpose, review of the client's technical security protocols and access controls, confirmation of liability insurance and contractual compliance capabilities, and on-site inspections of the client's facilities and systems. Companies also employ ongoing oversight mechanisms, including periodic audits, seeding of data files to detect unauthorized use or redistribution, and contractual provisions providing for consequences up to and including termination, financial penalties, and referral for prosecution in cases of contract violation or data misuse.*

G. Client Management

Effective, ongoing client management is equally important. The clients of data brokers come from a wide range of industries—advertisers, insurers, financial institutions, and law enforcement—that purchase or license data for equally diverse purposes. However, not all clients operate under the same legal obligations or ethical standards. Therefore, without robust policies for client management, data brokers cannot be effective stewards of consumer data.

To exhibit robust data stewardship, data brokers must implement monitoring processes that extend beyond initial client verification. Once a client is approved, data brokers should limit client access to approved uses and stated purposes. For example, a client who receives personal information for fraud prevention purposes should not be able to use that data for marketing without prior approval. If a client violates the terms of the sale or licencing agreement, data brokers should reserve the right to suspend or terminate the relationship. By ensuring clients' data use aligns with legal and ethical expectations, data brokers can reduce risk and protect individuals' personal information from downstream harms. In an environment where data is transferred through complex systems, responsible management of clients is a strategic imperative.

Case Study

- ***Transaction Monitoring and Audit –*** *One organization has implemented an automated internal review process that detects changes in client or user transaction patterns for volume, product type, and search criteria. Pattern changes trigger internal notification and account reviews. Additionally, random audits are performed requiring customers to provide certification of purpose and need. Failed audits trigger remediation up to and including account suspension or termination.*

Policy Takeaway

- In a data-driven economy, data brokers should proactively adopt—and policymakers should incentivize—robust data stewardship practices, which include organizational accountability measures, meaningful transparency, consumer choice mechanisms, robust cybersecurity measures, and due diligence strategies to vet third-party recipients of data and ensure appropriate and beneficial downstream uses of personal data.

REFERENCES

1. CIPL and BKL Discussion Paper – The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society (December 6, 2024), available at https://www.informationpolicycentre.com/resources/the-limitations-of-consent-as-a-legal-basis-for-data-processing-in-the-digital-society/.

2. *Id*.

3. CIPL White Paper – Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploring of Potential Effects (August 16, 2024), available at https://www.informationpolicycentre.com/resources/data-minimization-in-the-united-states-emerging-privacy-landscape-comparative-analysis-and-exploration-of-potential-effects-2/.

4. CIPL White Paper – Reconciling AI with the Data Minimization Principle: Bridging the Innovation and Privacy Gap (December 3, 2025), available at https://www.informationpolicycentre.com/resources/reconciling-ai-with-the-data-minimization-principle-bridging-the-innovation-and-privacy-gap/.

5. CIPL White Paper – Privacy-enhancing technologies and privacy-preserving technologies (PPTs): Understanding the Role of PETs and PPTs in the Digital Age (December 12, 2023), available at https://www.informationpolicycentre.com/resources/privacy-enhancing-and-privacy-preserving-technologies-understanding-the-role-of-pets-and-ppts-in-the-digital-age/.

6. CIPL White Paper - What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework (May 27, 2020), available at https://www.informationpolicycentre.com/resources/what-good-and-effective-data-privacy-accountability-looks-like-mapping-organizations-practices-to-the-cipl-accountability-framework/.

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.