Centre for Information Policy Leadership
HUNTON

Data Brokers in the Digital Economy: Toward Responsible Data Stewardship and Effective Regulation

Key Takeaways | June 2026

Takeaways from CIPL Roundtable

Data Brokers in the Digital Economy: Toward Responsible Data Stewardship and Effective Regulation

Held 20 May 2026

Washington, D.C.

On May 20, 2026, the Centre for Information Policy Leadership (CIPL) hosted an interactive roundtable to examine the data broker landscape. Aided by CIPL's recently published three-part **Policy Series on Data Brokers in the U.S.**,[1] we examined the challenges posed by the current regulatory environment; the need for proportionate, regulatory solutions to promote beneficial use cases; and potential avenues for incentivizing robust data stewardship measures.

Participants included senior professionals from CIPL member companies, along with representatives from federal and state agencies, state legislatures, and academia. The event, held at CIPL's Washington, DC office, was conducted under the **Chatham House Rule** to foster open and candid dialogue.

CIPL is pleased to share the following takeaways:

- ➔ **The data broker ecosystem is a complex, data sharing network that provides real (albeit hidden) consumer benefits.** Online banking and financial transactions services, social benefit and government assistance resources, and identity verification and anti-fraud protections are just a few of the many beneficial services that are reinforced by an invisible but necessary network of responsible data sharing. While the public's attention is understandably captured by harmful data sharing practices that can result in threats to safety and civil liberties, beneficial use cases are not widely recognized or understood. But as use cases are explained and consumers understand how data is being used, consumers are more likely to permit the use of their data for such beneficial uses.

- ➔ **What's in a name?** Data brokers are defined differently in a fast-growing number of state and federal laws, which address a wide spectrum of activities and business models (e.g. "selling", "sharing", or "processing" third-party *or* first-party data). Many companies not principally engaged in the brokerage of data can inadvertently fall within scope.

---

[1] CIPL published three discussion drafts in advance of the roundtable:

- *Understanding Data Brokers: Definitions, Regulations, and Enforcement in the United States*, available at https://www.informationpolicycentre.com/resources/understanding-data-brokers-definitions-regulations-and-enforcement-in-the-united-states-discussion-draft/.
- *Data Brokers and Proportionate Regulation: Balancing Commercial Value, Consumer Protection, and Civil Rights*, available at https://www.informationpolicycentre.com/resources/data-brokers-and-proportionate-regulation-balancing-commercial-value-consumer-protection-and-civil-rights/.
- *Data Stewardship and Accountability: Operationalizing Responsible Data Broker Practices*, available at https://www.informationpolicycentre.com/resources/data-stewardship-and-accountability-operationalizing-responsible-data-broker-practices-discussion-draft/.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

- **Motivations for regulating brokers differ widely.** At the state level, legislative efforts have focused on improving transparency via data broker registry laws and protecting sensitive consumer data (such as home addresses and geolocation information). For example, New Jersey's Daniel's Law—which protects the home addresses of active or retired judges, prosecutors, law enforcement officers, and their immediate family members—was enacted in response to the tragic killing of Daniel Anderl, the son of a United States District Court judge. The 2025 shooting that killed Minnesota state representative Melissa Hortman and her husband, Mark, and injured Minnesota state senator John Hoffman and his wife, Yvette, has further motivated legislators to regulate data brokers, as the Minnesota shooter purportedly relied on people search websites to identify the home addresses of public officials. While many state-level data registry laws include registration fees, a Maryland bill went a step further and attempted to tax the gross revenue of registered data brokers.

- **A risk-based approach can help differentiate helpful from harmful practices.** The data broker ecosystem includes a variety of business models and practices. A risk-based regulatory approach that includes impact assessments can enable high-value, low-risk practices while ensuring that high-risk practices satisfy enhanced compliance and oversight mechanisms. Such an approach will require multistakeholder development of risk scoring frameworks.

- **Regulators are concerned with conduct.** While regulators care about corporate principles and governance, they also consider how these are implemented when assessing the lawfulness of data broker practices.

- **Consumers do not want to be surprised.** Policymakers, regulators, and industry leaders agree that real people underly the data, and their interests must be considered at all times.

- **Responsible data brokers view organizational accountability as a competitive advantage.** CIPL member companies that engage in data broker activities see organizational accountability practices—such as transparency, impact/risk assessments, and security safeguards—as a business enabler. They have proactively embraced organizational accountability principles and robust cybersecurity measures. They apply know-your-customer principles and due diligence strategies to vet third-party recipients.

- **B2B customers oftentimes seek outcomes, not data.** Customers of business-to-business (B2B) data brokerage services frequently seek timely answers to specific questions: Is this individual who she says she is? Does this person own the property about which he is making a claim? Does this credit card belong to this user? Is this transaction valid? The services offered by data brokers can help answer questions such as these.

- **Explore the possibility of recognizing safe harbors.** Companies who are already doing the right thing should be duly recognized with regulatory safe harbors. Safe harbors can also incentivize industry-wide best practices and good behavior that preserves beneficial data sharing while preventing harmful practices and business models.

- **Legislators and regulators welcome engagement with industry.** Legislators tire of lobbyists looking merely for exemptions, but they welcome conversations with industry representatives who can educate them on best practices and help them craft outcomes- and risk-based

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

solutions. All stakeholders, including consumers, benefit from continued multi-stakeholder dialogue on matters related to the data broker ecosystem.

NEXT STEPS: CIPL will update its discussion drafts in light of this productive conversation, and we will schedule additional opportunities for stakeholder engagement. If you'd like to participate in future discussions, please contact us.

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.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.