Data Brokers: A Call To Action

NOVEMBER 2023

ASPEN TECH POLICY HUB
aspen institute

Image by Nasa at Unsplash

Introduction

The data brokerage industry – a catchall term for businesses that collect, process, store, and sell individualized personal data[1] – offers a number of services its customers find valuable, such as identity verification, fraud detection, and hyper-individualized marketing. Data brokers power these services by purchasing or collecting information from sources as disparate as court records, web browsers, apps, and mobile devices, and then aggregating that information for sale on the commercial market.

The amount of information data brokers collect – and the insights they develop from it – can be staggering. By pairing publicly available information with data from devices, data brokers have developed insights on hundreds of millions of American consumers, which can be as specific as the type of car they drive or the existence of ailments they may have such as depression or diabetes. Data brokers can even determine whether consumers fall into a financially vulnerable category such as "Rural and Barely Making It," "Tough Start: Young Single Parents," or "Credit Crunched: City Families."[2]

However, the consumers whose information powers this industry are largely unaware of what data brokers are, what information these companies collect, and the ways in which that information is used. Moreover, while federal policymakers have expressed concerns for decades about the lack of transparency and potential for harm this industry poses, the modern data brokerage industry still operates largely in the absence of government oversight.[3] Without further regulation and oversight, the harms that data brokerage poses to civil rights, national security, and consumer privacy may outweigh the benefits this industry offers.

To address this critical issue, the Aspen Institute's Tech Policy Hub convened an intergenerational, cross-disciplinary group of data privacy professionals in June 2023. This roundtable brought together leaders from government, academia, the private sector, and civil society. The purposes of this meeting were to discuss the challenges this industry poses and to propose steps that federal, state, and private actors can take to increase transparency and privacy protections in the data brokerage industry. The meeting was conducted under the Chatham House Rule to allow participants to speak freely.

This report summarizes the results of that collaboration. It discusses 4 areas that roundtable participants identified as opportunities for immediate action by federal and state policymakers:

- **Managing the Government's Use of Data Broker Services,** in recognition that government bodies at the federal, state, and local levels have increasingly turned to commercial data vendors as clients;
- **Limiting the Use of Data Brokers in Law Enforcement,** to mitigate the civil liberties and civil rights threats associated with data brokerage;
- **Enforcing Existing Laws to Combat Data Broker Abuses,** to remediate and to deter violations of consumer protection, anti-discrimination, and other laws; and
- **Educating the Public about Data Brokerage,** as a critical step to support informed policymaking and to empower individuals to exercise their privacy rights.

The report offers recommended actions that policymakers can take in each of these areas to increase protections for consumers and to mitigate the harms posed by data brokerage.[4] Crucially, these recommendations are tailored to be actionable ***without*** new federal legislation or regulations — providing an opportunity for policymakers to make an immediate impact on these critical issue.

This report is authored by the Aspen Tech Policy Hub staff. We would specifically like to thank Andrew Lewis for primary authorship of this report and for overall project leadership; Betsy Cooper and Mai Sistla for their thought leadership; Emma Calkins, B Cavello, Kateri Gajadhar-Smith, Constance Moore, and Gavin Victor for their critical support during the roundtable; and all of the roundtable participants.

Executive Summary

Key Recommendations for Policy Action

During the Aspen Institute's data brokers roundtable, participants were challenged to propose policy actions that – in the absence of comprehensive federal legislation or regulations imposing broad standards and restrictions on the data brokerage industry – could mitigate some of the privacy and civil liberties concerns associated with the commercial sale of personal data. Within that framework, attendees identified the following priority issues that policymakers have an opportunity to address using existing legal authorities:

Managing the Government's Use of Data Brokers

- **Limit the government's reliance on data brokers.** The White House and the Office of Management and Budget (OMB) could take action to curb the federal government's use of commercial data services, thereby increasing transparency and accountability. Recommendations include OMB exploring building in-house information systems, and the White House issuing standards to limit the use of data brokerage services with federal funds.
- **Increase transparency into the government's use of data brokerage services.** The lack of clarity on the federal government's use of data brokers is an obstacle to informed policymaking regarding the industry. In response, the White House could require all federal agencies to disclose contracts with data brokers, or federal grantors, such as the Department of Justice (DOJ), could require such disclosure from recipients of federal funds.
- **Promulgate standards for the protection of privacy and civil liberties.** The White House and OMB have the power to set government-wide standards for privacy and civil liberties protections, transparency, and data security in the federal government's use of data broker services. Through executive orders or memoranda to department heads, the federal government could lead the way in the responsible use of commercial data by setting standards that the overall industry could adopt, and by raising the bar for the parts of the industry that directly serve the federal government.

Photo by Adras Vas on Unsplash

Limiting the Use of Data Brokers in Law Enforcement

- **Restrict the use of commercial data for law enforcement purposes.** Serious constitutional and civil liberties concerns are associated with using data broker services to obtain personal information without obtaining a warrant or initiating other due process procedures. The White House, as well as DOJ and other federal law enforcement agencies, could impose restrictions on how commercial data may be used for law enforcement purposes. Suggested restrictions range from a wholesale ban on such uses to mandatory disclosure requirements and standards for law enforcement uses of commercial data, including when state and local governments purchase data broker services with federal funds.

Enforcing Existing Laws to Combat Data Broker Abuses

- **Limit the kinds of data that may be purchased and sold.** The Consumer Financial Protection Bureau (CFPB) could use its authorities under the Fair Credit Reporting Act to limit the personal information that credit reporting companies may sell on the commercial market.
- **Prioritize enforcement actions against data brokers.** The Federal Trade Commission (FTC), the Department of Housing and Urban Development, and other agencies responsible for enforcement of consumer protection and civil rights laws could prioritize filing enforcement actions against data brokers that engage in unfair, deceptive, or discriminatory acts or practices.

Educating the Public about Data Brokerage

- **Support research into the data broker industry.** Federal agencies such as DOJ and the National Science Foundation could support informed policymaking by conducting their own research into the data brokerage industry and by funding academic and nonprofit research into the industry's practices and effects.
- **Inform the public on its privacy-related rights.** Policymakers in the White House, at the CFPB, and at state level consumer protection agencies could partner with civil society organizations to enhance privacy protections by educating the public on how to exercise its existing rights, such as under state and federal "opt out" laws.

Image by Pawel Czerwinski at Unsplash

Recommendations on Managing the Government Use of Data Brokers

Among the broad categories of clients that the data brokerage industry serves – including hedge funds, real estate companies, and marketers – one stands out: the federal government. Federal agencies such as the Department of Homeland Security (and its component agencies, including Customs and Border Protection and Immigration and Customs Enforcement), the Federal Bureau of Investigation, and military and foreign intelligence agencies, routinely purchase the personal electronic data of Americans, including location data, on the commercial market.[5]

While a complex legal framework limits how law enforcement and intelligence agencies can access digital communications and other personal data outside of formal legal processes, existing law does not address the government's purchase of sensitive information from data brokers.[6] Moreover, there is currently no uniform policy governing the federal government's purchase of data brokerage services overall. Participants suggested that by addressing these gaps, federal policymakers have an opportunity to lead the way in mitigating the privacy and civil liberties concerns associated with data brokerage.

The White House

The White House, through its ability to set uniform federal policies and establish priorities for the whole of government, could be a central actor in making immediate strides in addressing the harms of data brokerage. Whether through executive orders or by exercising its convening power to motivate private action, participants identified several avenues for the White House to shape how the federal government uses data brokerage services:

- **The White House could issue an executive order limiting state, tribal, local, and territorial governments' use of services from data brokers when purchased with federal funds.** This could include restrictions on the use of Byrne discretionary funds, which the federal government awards to communities to improve the capacity of local justice systems, and restrictions on other support to state, tribal, local, and territorial law enforcement agencies, such as Justice Department grants.
- **The White House could issue an executive order instructing federal agencies to reevaluate their use of data brokerage services to increase transparency.** Participants identified two potential models for such reevaluations:
  - *The Privacy Act of 1974*, which requires Privacy Act Systems of Records Notices. These are public records that document government information systems that can identify individuals. These notices are currently only applicable to in-house government information systems. The White House could mandate that federal agencies issue Systems of Records Notices to document federal use of data brokerage services.
  - *The Computer Matching and Privacy Protection Act of 1988,* which requires Computer Matching Agreements. These are written agreements documenting the sharing of personally identifiable information (PII) between a federal agency and another federal or state body, and establishing safeguards for protecting the privacy of that PII. The White House could mandate that federal agencies agree to similar safeguards and public documentation when contracting for data brokerage services.
- **The White House could issue an executive order prohibiting the use of federal funds to purchase services from data brokers that fail to abide by Fair Information Practice[7] guidelines that are set out in the order.** In tandem with this order, the White House or another responsible agency could publicly list vendors that meet these guidelines and from which the government will purchase data brokerage services.
- **The White House could use its convening power to secure voluntary commitments from leading data brokerage companies** – such as Acxiom, Epsilon Data Management, Equifax, Experian, Oracle, and RELX – to adopt standards for the inclusion of certain error-prone data, like court record data, for decisionmaking in areas such as housing, employment, credit, and insurance.

Opportunity for State Level Action

A coalition of state attorneys general or state privacy agencies could convene data brokers in a similar way as the White House, or in tandem with federal efforts, to encourage vendors to adopt best practices for data brokerage.

Image by JJ Ying at Unsplash

Office of Management and Budget

Participants suggested that the Office of Management and Budget (OMB), which oversees the implementation of uniform executive policies across the federal government, could play a significant role in leading efforts to address the government's use of data brokers. Participants suggested that OMB's policy-setting authority could be exercised to increase transparency into the federal government's use of data broker services and to require privacy and civil liberties protections surrounding the use of those services.

- **OMB could issue a new circular or memorandum[8] on ensuring that data acquisition from data brokers is subject to Privacy Impact Assessments (PIAs) under the E-Government Act of 2002.** PIAs are public analyses that identify how federal agencies have incorporated privacy protections when they develop or procure new information technology involving the collection, maintenance, or dissemination of PII. Under current policy and practice, accessing data sold on the commercial market does not in all cases trigger the completion of a PIA under the E-Government Act; adding such a requirement would enhance transparency and ensure that brokered PII is as protected as in government-maintained systems.
- **Similarly, OMB could issue guidance governing how federal agencies procure data from brokers that is used to provide federal services or benefits.** Such guidance could address concerns such as mitigating biases present in commercially available data, or directing that data brokerage services follow data minimization requirements to win government contracts.
- **OMB could also explore options for establishing in-house fraud protection services for the use of the federal government.** Currently, the federal government contracts with third party data brokers to provide fraud protection services, such as the identity verification component of federal portals like Login.gov.[9] Especially if established with privacy safeguards, such as limitations on sharing PII across agencies, bringing fraud protection services in-house presents the opportunity for not just increased transparency, but also potential long term cost savings.
- **OMB could consult with the National Institute of Standards and Technology (NIST) to develop an efficacy and privacy certification for data brokerage.** Similar to current NIST information security requirements under the Federal Information Security Modernization Act[10], OMB could require that data broker services obtain this NIST certification as a prerequisite to acquiring federal contracts, particularly those involving law enforcement agencies. This would leverage the federal government's purchasing power to drive change throughout the data brokerage industry.
- **OMB could issue guidance requiring federal agencies to publicly report any contract to purchase or otherwise access commercial data.** These disclosures would increase transparency into the government's use of data brokerage services. In light of the sensitivities of data purchases for national security reasons, this directive could exempt certain defense or intelligence related data purchases from public disclosure.

Other Federal Agencies

Beyond the whole of government powers available to the White House and Office of Management and Budget, participants identified several actions that federal agencies could take within their own areas of authority to address data brokerage. Especially as clients of data broker services, and as the grantors of federal funds to state, tribal, local, and territorial governments to purchase those services for themselves, participants suggested that federal agencies could play a significant role in determining how data brokerage services are used, and under what conditions vendors may provide those services to the government.

- **The General Services Administration (GSA) could compile a database of all data broker vendors used by the federal government and make this information public.** At a minimum, the GSA database should include information on the identity of each vendor and a description of the services provided, with regular updates.
- **National security agencies could direct their privacy and civil rights officers[11] to review agency usage of data broker services and formalize a process for that usage.** Currently, the intelligence community lacks a set of guidance and procedures governing the use of data broker services, including guidance on how to protect privacy and civil liberties when using those services.[12]
- **The Department of Education could issue guidance clarifying that the Protection of Pupil Rights Amendment – a federal law affirming the rights of parents of minor students with regard to their children's educational records – limits the commercial use of student data.** Such guidance would clarify that school districts must establish policies to protect student privacy in the collection and sale of student data by companies that provide online services to K–12 students — and offer parents an opportunity to opt out of that collection and sale.

Opportunities for State Level Action

Many states have powers and authorities similar to those available at the federal level – and sometimes exceeding federal protections – which could be used to address data brokerage within their borders.

For example, state departments of education could use their own authorities, such as California's Student Online Personal Information Protection Act, to provide protections related to the collection, disclosure, and sale of the data of minor students.

State departments of economic development could also provide incentives to encourage data brokers and their clients to affirmatively provide opt-out or data deletion options for consumers.

Recommendations on the Use of Data Brokers for Law Enforcement Purposes

Because of the constitutional protections associated with both civil and criminal investigations and prosecutions, participants called out the use of brokered data for law enforcement purposes as raising unique concerns related to privacy and civil liberties.

In the wake of the Supreme Court's 2018 decision in *Carpenter v. United States*, which limited the government's ability to track an individual's cellphone location history, participants observed that many law enforcement agencies have increasingly turned to the commercial purchase of location and related data as an alternative to obtaining a warrant.[13] In light of this trend, participants suggested that federal law enforcement agencies could take immediate actions consistent with current law to address privacy and civil liberties concerns without compromising their public safety missions:

The White House

- **The White House could, through an executive order, direct federal law enforcement agencies to cease obtaining data from brokers for investigative or evidentiary purposes** without first obtaining a warrant or otherwise following due process. This order should not create new rights or benefits enforceable against the United States.
- **Alternatively, the White House could issue an executive order directing that the inspector general of each federal law enforcement agency conduct a review to certify that commercially obtained data fully comply with applicable privacy laws.** This mandatory review could be coupled with a moratorium on all law enforcement use of data broker services unless or until each relevant agency affirms its compliance with applicable privacy laws.

Department of Justice

- **The Department of Justice (DOJ) could update its digital evidence manual to state that data purchased from data brokers should not be permitted as evidence in a criminal prosecution** if it could not have been obtained with a warrant or other legal processes.[14] In addition to setting a baseline for federal prosecutions, this action would provide guidance to the state and local governments that rely on this manual in creating and updating their own procedures regarding digital evidence.
- **DOJ could issue guidance and provide technical assistance and training to state, tribal, local, and territorial law enforcement agencies regarding best practices for using commercial data.** This guidance and assistance would be focused on increasing public trust and enhancing public safety by incorporating privacy protections into the use of data brokerage services.
- **DOJ could issue a directive to state, tribal, local, and territorial law enforcement agencies requiring they issue a privacy impact statement when procuring data broker services with federal funds.** This privacy statement could disclose information about the data broker product, such as the size of the dataset or the sources of the information.
- **DOJ could require full disclosure of data broker vendors from all state, tribal, local, and territorial law enforcement agencies receiving federal funds.** The disclosure should specify the full range of surveillance and data broker products that grant recipients purchase using federal funds.

Opportunity for State Level Action

Participants suggested that state and municipal executives could issue their own orders governing the use of data broker services by their law enforcement agencies. Such orders could issue requirements such as mandating privacy reviews or privacy certifications from NIST or other national bodies as a contract requirement, or they could announce an outright ban on the use of these services for evidentiary or investigative purposes.

Image by Markus Spiske at Unsplash

Recommended Enforcement Actions under Existing Law

Participants identified several enforcement authorities under civil rights, consumer protection, and other laws that provide an avenue for enhancing transparency and protecting privacy in the data brokerage industry. Laws established to protect consumers against unfair or deceptive practices, promote fairness and transparency in the marketplace, and protect individuals from violations of civil rights laws can all be used to address some of the negative effects of the consumer data marketplace.

At the federal level, participants focused their recommendations on 2 key agencies with responsibility for the data brokerage industry: the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). Both agencies are actively considering their roles in ensuring that data brokers comply with the law.

The CFPB recently issued a call for public comment on the data broker industry and the collection and sale of consumer information, which could be an initial step in engaging in rulemaking under the Fair Credit Reporting Act and other statutory authorities regarding data brokers. And last year, the FTC sued a data broker for selling the geolocation data of individuals in a format that tracked movements to and from sensitive locations like reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.[15]

These recent actions demonstrate that federal enforcement authorities are willing to address the negative effects of data brokerage, and their continued action will help mitigate concerns with how these services can be abused.

Consumer Financial Protection Bureau

CFPB to Take Action to Protect against Harmful Data Brokerage Practices

In August 2023, prior to the publication of this report, CFPB Director Rohit Chopra announced that the CFPB expects to propose new rules under the Fair Credit Reporting Act to prevent misuse and abuse in the data brokerage industry. The CFPB is considering rulemaking to define data brokers that sell certain types of consumer data as "consumer reporting agencies," which would require them to take steps to ensure data accuracy and to prohibit misuse.

Chopra announced that the CFPB is also considering a proposal to clarify the extent to which "credit header data" constitutes a "consumer report," which would reduce the ability of credit reporting companies to disclose sensitive contact information.

Both proposals were discussed at the roundtable, and summaries of those suggestions are included in this report. The CFPB plans to release its proposal for a new rulemaking on these issues in 2024.

Participants focused on the Consumer Financial Protection Bureau's authorities under the Fair Credit Reporting Act (FCRA) to address harmful behavior by the data broker industry:

- **The CFPB could clarify and enforce Fair Credit Reporting Act violations against data brokers.**[16] Participants suggested that the CFPB's first step could be to issue an advisory opinion clarifying that "credit header" data – meaning personally identifying information found in a credit report, such as full name, current and former addresses, and current and former telephone numbers – are not exempt from regulations promulgated under the FCRA. Because credit header data are not currently regulated under the FCRA, this information can be sold in bulk by credit reporting agencies. The CFPB's action here would enhance consumer privacy by limiting the circumstances in which credit reporting agencies can sell those data.
- **The CFPB could publish an advisory opinion or policy statement clarifying the types of data that may be included in consumer reports under the FCRA.** For example, the CFPB could more precisely identify what kinds of data constitute "medical information," which is generally prohibited from inclusion in consumer reports.

Federal Trade Commission

Participants suggested that the Federal Trade Commission could engage in a number of actions under Section 5 of the Federal Trade Commission Act to initiate enforcement actions against unfair or deceptive acts or practices:

- **The FTC could issue a policy statement declaring certain data broker practices (e.g., selling precise geolocation) as being in violation of Section 5.** This could clarify or expand upon the positions the agency has taken in enforcement actions such as its August 2022 lawsuit against Kochava for selling geolocation data regarding sensitive locations, and its 2021 suit against Flo Health, a fertility tracking app that sold sensitive health data to third parties.
- **The FTC could begin issuing Notices of Penalty Offenses[17] to companies that disclose or reuse personal data outside of a consented context.** This would not only stop data brokers that currently deceptively disclose personal data, but also deter future abuses of customer consent.
- **The FTC could expand its public guidance on what constitutes a "substantial" injury under Section 5 to explicitly include privacy intrusions,** such as the deceptive sale of geolocation data or other highly sensitive forms of data. By doing so, the FTC could serve notice to data brokers that it considers such actions to be enforceable violations of Section 5.
- **The FTC could prioritize enforcement actions to combat a subset of the activities that use data brokerage services and engage in deceptive acts or practices.** Examples of potential priority actions include suits against vendors that deceptively market "unbiased" artificial intelligence tools that in practice produce unfair or discriminatory results; vendors that disclose or reuse data outside of a consented context;[18] or vendors that sell the personal information of consumers without verifying the data for accuracy.
- **The FTC could enforce FCRA violations as appropriate.** To the extent it has enforcement authority, the FTC could enforce violations of the Fair Credit Reporting Act against data brokers in conjunction with the CFPB.

Other Enforcement Agencies

Participants suggested that federal departments with broad civil rights enforcement responsibilities – such as the Department of Housing and Urban Development, DOJ, and the Equal Employment Opportunity Commission – could enforce existing civil rights laws against data brokers.

- Enforcement actions could target practices in which brokered data are used in processes that result in discriminatory outcomes, such as in tenant screening, moneylending, and hiring.[19]

- **Federal and state consumer protection agencies could partner with civil rights nonprofits to enforce noncompliance with opt-out rights.** Under federal law and some state laws, consumers must be notified that they may opt out of credit reporting companies sharing their personal information with companies like banks or insurers. Participants suggested that with the aid of consumer protection agencies, civil rights organizations and privacy focused nonprofits could initiate a campaign to test for companies' compliance with applicable state privacy laws by running a grassroots mass opt-out campaign encouraging consumers to use their opt-out rights under applicable state privacy laws. These organizations could then share the results of this campaign to state and federal enforcement agencies to aid enforcement actions.

Opportunity for State Level Action

Participants suggested that state attorneys general or consumer protection agencies could enforce existing state consumer protection laws to require licenses for data brokers. These licenses could require standards for data minimization, accuracy, and the regular updating or retiring of data. The licenses could be narrowly targeted to apply only to brokers that traffic in particularly concerning types of data, such as those that handle criminal records, court information, and other data related to the criminal justice system.

Image by Ian Battaglia at Unsplash

Increasing Public and Policymaker Understanding of the Data Broker Industry

Policymaking regarding the commercial data industry has moved slowly and incrementally over the decades, in part because of the lack of publicly available information on data brokers; their practices in collecting, analyzing, and selling data; the identity of their clients; and the sources of the data being bought and sold.

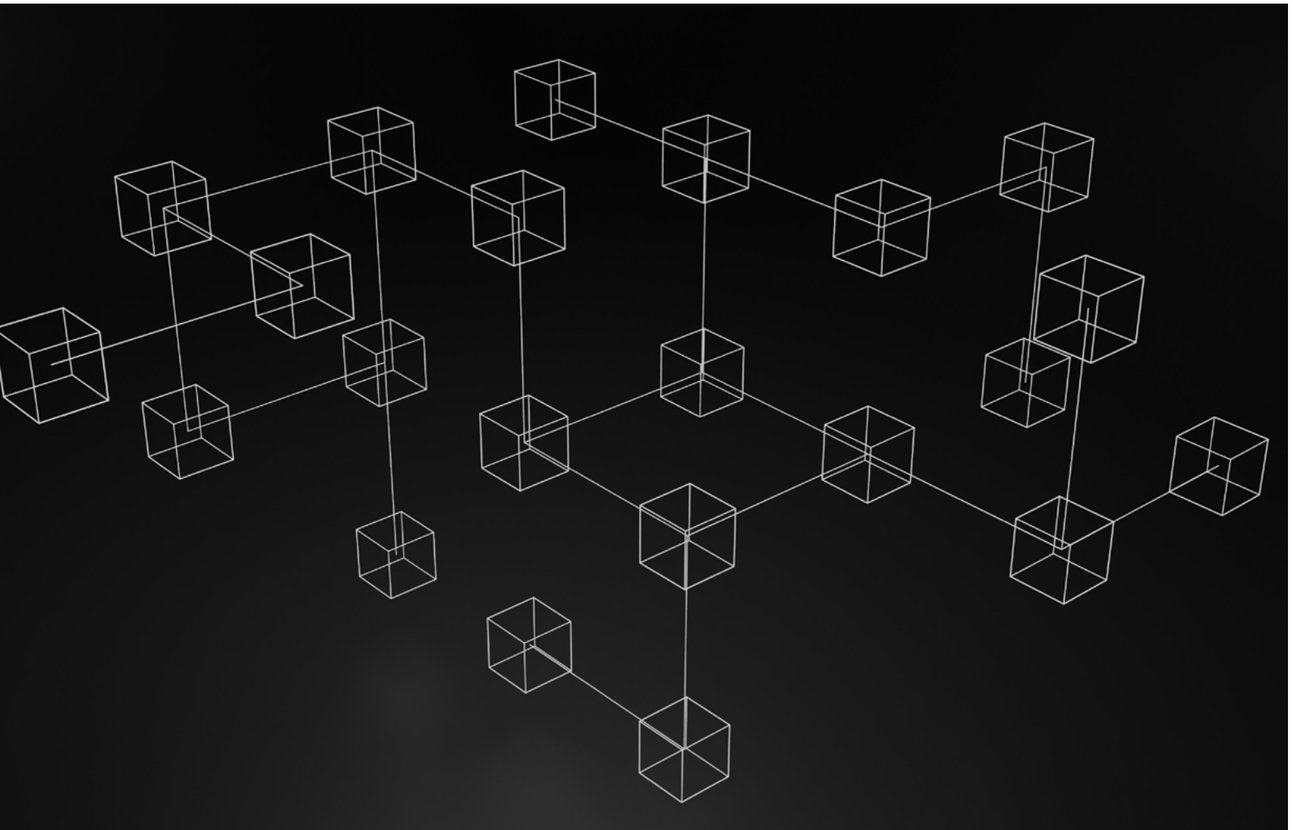
Participants said that one of the more significant challenges in developing the kind of public understanding of the industry that could inform policymaking is that data brokers rarely engage directly with the consumers whose data they collect and sell. While each data source may provide only a few elements about a consumer's activities, data brokers can analyze these data elements together to form a more detailed composite of the consumer's life.

Several participants argued that shedding more light on the data broker industry could be a critical step in ensuring that it develops with an appropriate recognition of its associated risks. Participants suggested the following actions for government bodies to take, some in partnership with civil society, to advance the public's education on data brokerage:

- **The White House or the FTC could publish a white paper that examines the role the industry plays across multiple areas of American life.** The Federal Trade Commission's 2016 report on "big data" could provide a model for offering a public assessment of the risks and benefits of the data broker industry, as could the Obama administration's May 2014 and May 2016 reports on big data.
- **The Department of Justice's Civil Rights Division could offer grants to**

organizations that are examining the civil rights and civil liberties impact of data brokers. These grants could be used to conduct research into the use of data brokerage services among law enforcement agencies across the country, and provide training and technical assistance to communities in the responsible use of these services.

- **Similarly, the National Science Foundation could provide grants for research on the cross-disciplinary impacts of data brokerage.** These grants could encourage research that captures the scope of data brokers' reach across a number of fields, such as medicine, education, consumer protections, and the legal system.
- **The Consumer Financial Protection Bureau, or state consumer protection agencies, could engage in public information campaigns on how to exercise privacy rights.** Examples could include public service announcements on how to exercise the opt-out right under the Fair Credit Reporting Act, or public guidance on how consumers may exercise their rights to access, correct, and delete their personal data under state law.



Conclusion

The participants of the roundtable on digital privacy and data brokers coalesced around a series of concerns and best practices for mitigating the harms this industry poses.

- ***First,*** and emphasized most often by participants, is that the federal government must act to increase transparency, accountability, and civil liberties protections regarding its own use of data broker services. The White House, OMB, and other federal departments could take the lead in instituting these efforts at a whole of government level.
- ***Second,*** participants underscored that limiting the government's use of data brokerage services among law enforcement agencies – particularly as an alternative to obtaining information according to legal processes – is one of the most urgent and significant steps it could take in ensuring that data brokers do not undermine civil liberties protections. The White House, the Department of Justice, and other federal law enforcement agencies could all take immediate steps to mitigate these concerns.
- ***Third,*** participants encouraged government actors with enforcement authorities, such as the CFPB and FTC, to prioritize enforcing existing laws prohibiting harmful data broker practices, especially as the industry continues to mature in technologically novel ways.
- ***Finally,*** participants suggested that policymakers – including the White House, DOJ, and state and federal consumer protection agencies – take the lead in educating the public about the data broker ecosystem, both to enable informed policymaking and to empower citizens in exercising their rights.

These suggested interventions are not a substitute for more comprehensive action through legislation or regulation. However, they present an opportunity for policymakers to make an immediate impact in shaping the data brokerage industry's growth and mitigating its associated risks. In taking action now, policymakers could shape the data broker ecosystem in ways that increase transparency, respect civil liberties, and empower individuals to shield their private information from becoming marketplace commodities.

Image by Shubham Dhage at Unsplash

Endnotes

1 "Data Brokers," Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/ (2023).

2 Staff of Senate Comm. on Commerce, Science, and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," at ii (December 18, 2013), https://www.commerce.senate.gov/services/files/0D2B3642-6221-4888-A631-08F2F255B577.

3 Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

4 The recommendations in this report do not reflect a "group consensus," but instead reflect themes, ideas, and recommendations that individual participants proposed and refined throughout the discussion. While no single participant would support every idea contributed through this process, all acknowledged the critical role that actors outside of the U.S. Congress can play in increasing accountability and privacy in the data brokerage industry.

5 Bennett Cyphers, "How the Federal Government Buys Our Cell Phone Location Data," *Deeplinks Blog*, Electronic Frontier Foundation (June 13, 2022), How the Federal Government Buys Our Cell Phone Location Data.

6 One cornerstone federal law addressing the federal government's access to sensitive information is the Electronic Communications Privacy Act of 1986, which protects certain communications from unauthorized interception or disclosure. The act does not prohibit data brokers from selling sensitive information to government agencies. See Carey Shenkman et al., *Legal Loopholes and Data for Dollars, Center for Democracy & Technology* (December 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

7 "Fair Information Practice Principles" are widely accepted principles that agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy. They provide the framework for privacy policies across the federal government. See Federal Privacy Council, "Fair Information Practice Principles (FIPPs)," https://www.fpc.gov/resources/fipps/; see also Robert Gellman, "Fair Information Practices: A Basic History – Version 2.22" (last revised April 6, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

8 An OMB circular is a document that provides standardized instructions and guidance to federal agencies on the implementation of federal law and policy across an array of policy areas and topics.

9 See Alfred Ng, "Data Brokers Raise Privacy Concerns — But Get Millions from the Federal Government," *Politico* (December 21, 2022), Data brokers raise privacy concerns — but get millions from the federal government.

10 See "Federal Information Security Modernization Act," Cybersecurity & Infrastructure Security Agency (2023), Federal Information Security Modernization Act | CISA.

11 Numerous federal laws establish privacy and civil rights/civil liberties officer positions within national security agencies such as the Central Intelligence Agency, the Department of Homeland Security, and the Office of the Director of National Intelligence. These officers are responsible for ensuring that the protection of privacy, civil rights, and civil liberties is appropriately incorporated into these agencies' operations. See, e.g., "Office of Civil Liberties, Privacy, and Transparency — Who We Are," Office of the Director of National Intelligence (2023), Office of Civil Liberties, Privacy and Transparency - Who We Are.

12 See Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information, "Report to the Director of National Intelligence" (January 27, 2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

13 See Chris Baumohl, "ODNI Report on Intelligence Agencies' Data Purchases Underscores Urgency of Reform," Electronic Privacy Information Center (July 7, 2023), https://epic.org/odni-report-on-intelligence-agencies-data-purchases-underscores-urgency-of-reform/.

14 DOJ's digital evidence manual serves as a baseline set of policies and procedures for law enforcement agencies at all levels of government regarding the collection, handling, and processing of digital evidence. The manual also plays a role in guiding law enforcement agencies through the accreditation process of the Commission on Accreditation for Law Enforcement Agencies. See National Institute of Justice, Digital Evidence Policies and Procedures Manual (May 2020), Digital Evidence Policies and Procedures Manual | National Institute of Justice.

15 FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations," Federal Trade Commission (August 29, 2022), FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations.

16 In a February 8, 2023, letter to the CFPB, privacy focused organizations such as the Electronic Privacy Information Center and the Center for Democracy & Technology called on the agency to take enforcement and regulatory actions to protect consumers from certain harmful and abusive practices of data brokers, such as buying and selling hundreds of millions of names and addresses gathered by essential utilities companies without consumers' knowledge or consent and trafficking in inaccurate data flowing from name mismatches. See Letter to Rohit Chopra, Director, CFPB, from Center for Democracy & Technology et al. (February 8, 2023), https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf.

17 Under the FTC's Penalty Offense authority, it can seek civil penalties against a company or individual if it proves that they knew that the FTC had already issued a written decision (after an administrative trial) against another entity that the same conduct was unfair or deceptive.

18 Such an action could use the FTC's suit against BetterHelp, an online counseling service that allegedly sold its customers' mental health information to third parties, as a model. See Lesley Fair, "FTC Says Online Counseling Service BetterHelp Pushed People into Handing Over Health Information — and Broke Its Privacy Promises," Business Blog, Federal Trade Commission (March 3, 2023), FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises.

19 This proposal is similar to a recent joint statement from the CFPB, DOJ's Civil Rights Division, the Equal Employment Opportunity Commission, and the FTC, declaring that existing legal authorities protecting civil rights, nondiscrimination, fair competition, and consumer protection apply to artificial intelligence systems. See Rohit Chopra et al., "Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems" (April 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.


ASPEN TECH
POLICY HUB