

ESSAY

PRIVACY IN PERIL:

WHEN UNCHECKED SURVEILLANCE POWER AND
UNBALANCED PRESIDENTIAL POWER COLLIDE

*Rebecca Kelly Slaughter**

I. INTRODUCTION: TWO CRISES CONVERGING	1214
II. DATA CONCENTRATION	1215
A. From Data Collection to Data Concentration	1215
B. The Surveillance Advertising Architecture	1218
C. Why Concentration Is a Problem, Not Just Collection	1220
III. EXECUTIVE POWER.....	1223
A. Expansion of the Power of the President over Government Institutions.....	1223
B. Executive Power and Data-Driven Markets.....	1225
C. Executive Power over Private Actors	1228
IV. THE THREAT MULTIPLIER: WHEN THE TWO PROBLEMS COLLIDE	1231
A. The Architecture of Coercion	1231
B. Government-as-Purchaser	1234
C. Tech-Titan-as-Political-Ally.....	1235
D. Precedent and Pattern: Historical Lessons	1236
V. THE INTERNATIONAL DIMENSION: AMERICAN DATA POWER HAS NO BORDERS	1238
A. US Platforms Hold the World's Data	1238

* Rebecca Kelly Slaughter was nominated by President Trump to serve as a Federal Trade Commissioner in 2018, and nominated for a second term by President Biden. She was unanimously confirmed by the United States Senate both times. She was fired by President Trump in March 2025 and challenged her removal in federal court. In June 2026, the Supreme Court decided *Trump v. Slaughter*, overturning nearly a century of precedent in finding that statutory removal restrictions violate the Constitution.

B. The Collapse of the United States as a Trusted Data Partner	1239
C. The Stakes for Democratic Dissent Globally.....	1242
VI. TOWARD A FRAMEWORK: WHAT MUST BE DONE	1243
A. Restore Independent Agency Protections.....	1243
B. Comprehensive Federal Privacy Legislation with Substantive and Structural Protections.....	1245
C. Limits on Data Concentration	1246
D. International Models and Cooperative Pressure.....	1247
VII. CONCLUSION: THE STAKES.....	1248

I. INTRODUCTION: TWO CRISES CONVERGING

I write this Essay as someone who has spent most of the last decade as a Federal Trade Commissioner, developing a deep understanding of the threats posed by the unchecked accumulation of personal data in the hands of a small number of dominant corporations. I write it also as the named plaintiff in *Trump v. Slaughter*,¹ a Supreme Court case decided in June 2026 in which the Court determined that the President of the United States may fire members of independent federal agencies at will, notwithstanding ninety years of constitutional precedent² and over a century of clear statutory language³ that said he may not. I sit at the convergence of different areas of substantive law—privacy and competition on the one hand, administrative and constitutional law on the other—which has given me a unique perspective on their interaction.

The continued unfettered commercial agglomeration of data, especially in the hands of concentrated corporate giants, and the simultaneous expansion of presidential power—including over agencies Congress designed to have a degree of independence—

1. See *Trump v. Slaughter*, 146 S. Ct. 2883 (2026). The US District Court for the District of Columbia held my removal unlawful and reinstated me. See *Slaughter v. Trump*, No. 25-cv-00909, 2025 WL 1984396 (D.D.C. July 17, 2025). The Supreme Court granted certiorari before judgment and stayed the lower court's order. See *Slaughter*, 146 S. Ct. at 2883 (overturning *Humphrey's Executor v. United States*, 295 U.S. 602 (1935), and holding that the Federal Trade Commission's ("FTC") for-cause removal provision is contrary to the separation of powers, and that the President may remove FTC Commissioners at will).

2. *Humphrey's Executor v. United States*, 295 U.S. 602 (1935).

3. 15 U.S.C. § 41.

are mutually reinforcing crises that together create a threat to personal privacy qualitatively different from, and far more dangerous than, either poses alone. When massive troves of data are held by very few corporations, and when the government is willing and increasingly able to strong-arm those corporations, personal privacy is imperiled.

This Essay proceeds in six parts. Section II traces the current state of data concentration: a surveillance economy in which a handful of platforms and brokers hold granular, persistent, and comprehensive information about virtually every person in the country. Section III examines the ways in which the Trump administration has expanded the power of the President over both government institutions and private market actors. Section IV shows how these two developments in combination create an architecture of coercion, in which an unconstrained presidency can leverage corporate data holdings as instruments of political control. Section V explains the extraterritorial consequences of this dynamic: because the data held by American platforms is not bounded by American borders, the deconstruction of American regulatory institutions threatens both the privacy of people worldwide and international data flows. Section VI sketches some of the reforms necessary to address these converging crises.

II. DATA CONCENTRATION

A. *From Data Collection to Data Concentration*

The story of American data privacy over the past quarter century is simultaneously a story about concentration. Data collection by commercial actors is not new. Credit bureaus have compiled financial histories for decades; direct marketers have maintained customer lists since the postwar era; consumer reporting agencies have aggregated behavioral records since before the internet.⁴ What changed in the digital era was not merely the scale of collection, but its structure: While there

4. The Fair Credit Reporting Act established the first comprehensive federal regulation of consumer data held by credit reporting agencies. *See* 15 U.S.C. §§ 1681–1681x. It was enacted in response to the longstanding practice of credit bureaus compiling financial histories on American consumers without their knowledge or consent. *See* *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001) (describing business practices of credit bureaus).

continues to be a wide range of companies that are incentivized to engage in expansive data collection, a small number of platforms now occupy positions of extraordinary dominance over the flow of personal information, through a combination of organic growth and aggressive acquisition.⁵

During my time at the Federal Trade Commission (“FTC”), we saw extensive evidence of unrestrained accumulation of personal data. The Commission brought cases involving the illegal collection or use of data against Facebook/Meta,⁶ Google/Alphabet,⁷ Amazon,⁸ and many other smaller companies.⁹ Data collection and

5. See, e.g., Tom Wheeler, *Big Tech Won. Now What?*, BROOKINGS (Oct. 16, 2023), <https://www.brookings.edu/articles/big-tech-won-now-what/> [<https://perma.cc/RK8B-3YUE>]; see also Chris Alcantara et al., *How Big Tech Got So Big: Hundreds of Acquisitions*, WASH. POST (Sept. 26, 2023), <https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/> [<https://perma.cc/5GS3-54VM>]; FED. TRADE COMM’N, NON-HSR REPORTED ACQUISITIONS BY SELECT TECHNOLOGY PLATFORMS, 2010–2019: AN FTC STUDY (Sept. 2021), <https://www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf> [<https://perma.cc/2WHC-HAX5>] [hereinafter NON-HSR STUDY].

6. See *United States v. Facebook, Inc.*, No. 19-cv-2184, ECF No. 38-1 (D.D.C. May 31, 2023) (imposing five billion dollar civil penalty for violations of 2012 FTC order); see also Press Release, Fed. Trade Comm’n, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> [<https://perma.cc/4JL4-X3LP>] [hereinafter Facebook Press Release]; Dissenting Statement of Commissioner Rebecca Kelly Slaughter In the Matter of FTC v. Facebook (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf [<https://perma.cc/JS9X-8YWT>] [hereinafter Slaughter Facebook Dissent].

7. See *United States v. Google LLC*, No. 19-cv-02642-BAH, ECF No. 1 (D.D.C. Sept. 4, 2019) (settling for US\$170 million civil penalty for Children’s Online Privacy Protection Act (“COPPA”) violations); see also Press Release, Fed. Trade Comm’n, Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law (Sept. 4, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law> [<https://perma.cc/RE9A-6ZZ4>].

8. See *United States v. Amazon.com, Inc.*, No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023) (imposing twenty-five million dollar civil penalty for violations of COPPA Rule through Alexa’s data retention practices); see also Press Release, Fed. Trade Comm’n, FTC and DOJ Charge Amazon with Violating Children’s Privacy Law by Keeping Kids’ Alexa Voice Recordings Forever (May 31, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever> [<https://perma.cc/FY69-4TZU>].

9. See generally Press Release, Fed. Trade Comm’n, FTC Releases 2023 Privacy and Data Security Update (Mar. 28, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update> [<https://perma.cc/4XJS-LBE2>].

misuse were also something the Commission studied with input from the market. In 2021, the FTC published a study documenting the data collected by internet service providers,¹⁰ and, in 2022, we opened a rulemaking record on the topic of Data Security and Commercial Surveillance.¹¹ That record, all of which remains publicly available, provides documentation from divergent perspectives—industry, academia, civil society—many of which disagree about whether indiscriminate data collection is a problem, but almost all of which agree it is happening.¹²

The result, by any serious measure, is an economy in which we don't even know about many of the companies that know everything about us. To navigate modern life, a person may, in the course of an ordinary day, generate data that flows to an overlapping set of corporate holders. This happens every time one communicates by email or text, searches the web, uses a digital map, shops online, visits a doctor, drives a connected vehicle, or simply carries a smartphone. These data holders know not only what you bought, but where you went, whom you called, what you searched for, what health conditions you researched, what political content you engaged with, and how your behavior has changed over time. That data is used in turn to make decisions for and about

10. See FED. TRADE COMM'N, A LOOK AT WHAT ISPS KNOW ABOUT YOU: EXAMINING THE PRIVACY PRACTICES OF SIX MAJOR INTERNET SERVICE PROVIDERS (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf [<https://perma.cc/N2G2-WA7D>]. The study was conducted pursuant to Section 6(b) of the FTC Act through orders issued in 2019 to AT&T, Charter, Comcast, Verizon, T-Mobile, and Google Fiber. See 15 U.S.C. § 46(b).

11. See Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (proposed Aug. 22, 2022); see also Statement of Commissioner Rebecca Kelly Slaughter Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20ANPR%20Statement%2008112022.pdf [<https://perma.cc/F5YQ-LM9D>].

12. The rulemaking docket for 87 Fed. Reg. 51,273 is available at Trade Regulation Rule on Commercial Surveillance and Data Security, REGULATIONS.GOV, <https://www.regulations.gov/document/FTC-2022-0053-0414> [<https://perma.cc/8YNR-CTV7>]. During the comment period, the FTC received over 11,000 public comments from industry, consumer advocates, academics, and civil society organizations. See *id.* Comments ranged from industry submissions arguing that existing enforcement was adequate, see, e.g., Chamber of Com. of the U.S., Comment Letter on Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security (FTC-2022-0053-0889), to consumer advocacy submissions arguing that broad prohibitions on data collection were necessary, see, e.g., Elec. Priv. Info. Ctr., Comment Letter on Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security (FTC-2022-0053-0879).

you, such as what information you get to see and what price you pay for goods. That is why I prefer the term “data abuses” over “data privacy violations” to describe the potential harms that can flow from unlimited data collection.¹³

B. *The Surveillance Advertising Architecture*

The business model that drives this concentration is surveillance advertising: the pervasive collection and use of consumer data to enable micro-targeted behavioral advertising, usually offered in exchange for ostensibly free digital services.¹⁴ The notice-and-consent framework that has largely governed American privacy law for two decades is fundamentally inadequate to address it.¹⁵ The notice-and-consent framework works in a world of discrete permissioned transactions. It is not equipped for an economy in which data is aggregated at scale, used to build detailed inferences about sensitive characteristics such as health, religion, political affiliation, and sexual orientation, and held in forms accessible to a government that has both the motive and, increasingly, the means to compel or coerce access.

The FTC’s data broker enforcement actions in recent years offer a window into how far the surveillance advertising architecture has extended. In December 2024, the Commission took action against Gravy Analytics and its subsidiary Venntel, alleging that these companies had collected, processed, and curated more than seventeen billion location signals from around

13. See Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law* (Sept. 7, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf [<https://perma.cc/UH8Z-ZYZ4>].

14. See MATTHEW CRAIN, PROFIT OVER PRIVACY: HOW SURVEILLANCE ADVERTISING CONQUERED THE INTERNET (2021); see also Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28 NEW LAB. F. 10 (2019).

15. See Slaughter, *supra* note 13 (laying out detailed critique of this model); see also Public Statement of Commissioner Rebecca Kelly Slaughter As Prepared for Delivery, Disputing the Dogmas of Surveillance Advertising (Oct. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597050/commissioner_slaughter_national_advertising_division_10-1-2021_keynote_address.pdf [<https://perma.cc/7P2W-NQTZ>]. The market evolutions over the intervening years have only strengthened my view that notice and choice is an unworkable model for dealing with data in the digital age. See *id.*

one billion mobile devices daily.¹⁶ Gravy Analytics had appended over one thousand behavioral labels to individual consumers, tracking attendance at religious services, visits to reproductive health clinics, participation in political events. It then sold these profiles to private companies and government agencies alike.¹⁷ The companion action against Mobilewalla revealed similar practices: raw location data on consumers compiled based on real-time bidding (“RTB”) data, without meaningful consent, sold to a chain of downstream buyers who used it to identify individuals at sensitive locations including military installations, domestic violence shelters, and union organizing events.¹⁸

The Commission also sued Kochava, a data broker the agency alleged sold sensitive data on consumers including:

[P]recise geolocation data and a ‘staggering amount of sensitive and identifying information,’ including device users’ ‘names, MAIDs, addresses, phone numbers, email addresses, gender, age, ethnicity, yearly income, economic stability, marital status, education level, political affiliation, ‘app affinity’ (*i.e.* what apps consumers have installed on their phones), app usage,’ and ‘interests and behaviors.’¹⁹

In its rejection of Kochava’s motion to dismiss, the District Court explained that “selling ‘massive amounts of private and

16. See Press Release, Fed. Trade Comm’n, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites (Dec. 3, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers> [<https://perma.cc/ZPT8-9SHB>] [hereinafter Gravy Analytics Press Release].

17. See Statement of Commissioner Alvaro M. Bedoya Joined by Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter in full, and Commissioner Melissa Holyoak in Part I, In the Matter of Gravy Analytics, Inc. & Venntel, Inc. (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-gravy-statement.pdf [<https://perma.cc/ZE96-J9WZ>] [hereinafter Bedoya Statement] (describing how Venntel’s customers included federal agencies such as the Department of Homeland Security, the Drug Enforcement Administration, the FBI, and the IRS).

18. See Press Release, Fed. Trade Comm’n, FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data (Dec. 3, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data> [<https://perma.cc/2F8B-NZDR>] [hereinafter Mobilewalla Press Release].

19. See Memorandum Decision and Order at 5, *FTC v. Kochava, Inc.*, No. 2:22-cv-00377-BLW (D. Idaho Feb. 3, 2024) (denying Kochava’s motion to dismiss).

encyclopedic information’ that puts consumers at a significant risk of suffering secondary harms” can plausibly cause substantial injury.²⁰ The court also held that, independently, Kochava’s “alleged invasion of privacy—which is substantial both in quantity and quality—plausibly constitutes a ‘substantial injury’ to consumers.”²¹ These law violations are the logical products of the data economy business model, which incentivizes collection of as much data as possible. The incentive has only increased in the age of AI, which demands extensive data input to train models.

C. Why Concentration Is a Problem, Not Just Collection

Even as companies of all sizes have been indiscriminately collecting data, some of the largest players in the industry have been getting larger, which means they control even more vast troves of data.²² Competition law has been the primary lens for examining the market power of large digital services companies, but it has not been successful in checking that power. Notwithstanding aggressive enforcement efforts that began in the first Trump administration and picked up steam through the Biden administration,²³ the size and power of these tech giants have only

20. *See id.* at 10.

21. *See id.* at 13. The FTC settled its case against Kochava in June 2026. *See* Press Release, Fed. Trade Comm’n, FTC to Ban Kochava and Subsidiary from Selling Sensitive Location Data to Settle Charges They Sold Location Data Linked to Millions of Mobile Devices (May 4, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/05/ftc-ban-kochava-subsidiary-selling-sensitive-location-data-settle-charges-they-sold-location-data> [<https://perma.cc/BY34-EA6L>].

22. In 2021, the Commission published a study of unreported acquisitions by a select group of major technology platforms between 2010 and 2019. *See* Press Release, Fed. Trade Comm’n, FTC Staff Presents Report on Nearly a Decade of Unreported Acquisitions by the Biggest Technology Companies (Sept. 15, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-staff-presents-report-nearly-decade-unreported-acquisitions-biggest-technology-companies> [<https://perma.cc/8KKL-KC8L>]. That study revealed that these companies had collectively completed hundreds of acquisitions that fell below the Hart-Scott-Rodino reporting thresholds and thus were never reviewed for competitive harm or subjected to public scrutiny, and yet served systematically to expand the data holdings of already-dominant firms. *See id.* Each acquisition was, in isolation, arguably modest. In aggregate, they represented a deliberate and largely invisible strategy of accumulating market power in businesses that were largely built on the collection of personal data. *See id.*

23. *See, e.g.,* United States v. Google LLC, No. 20-cv-03010 (D.D.C. Sept. 2, 2025) (Department of Justice (“DOJ”) antitrust suit filed Oct. 20, 2020; court found Google liable for illegal monopoly in search and search advertising, Aug. 5, 2024); FTC v. Meta Platforms,

grown.²⁴ Current competition law is subject to multiple limitations: Enforcement that commences after violations have occurred can struggle to disentrench market power both practically and legally; cramped jurisprudential interpretations of the law tend to favor exculpatory explanations over evidence of harm, and even where liability is determined, remedies are limited and ineffective.²⁵ While competition law allows consideration of a wide range of input and output market harms, including effects on innovation and quality, it is most responsive to demonstrable changes in price and output.²⁶ Though harder to quantify, loss of privacy is one substantial quality effect of concentrated markets.²⁷

Zooming in on the data governance implications of the market power of large tech platforms, a disturbing picture emerges. Competition and consumer protection law are generally deeply intertwined, but nowhere is their connection more vivid than in the data privacy context. Concentration matters for privacy because it changes the stakes of collection in at least three ways.

First, concentration makes avoidance impossible. In a competitively healthy market, a consumer who objects to one firm's data practices can, at least theoretically, patronize a more privacy-protective rival, limiting the power of and data accessed by the offensive firm.²⁸ When the market is dominated by only two or three firms, switching opportunities are limited. This is especially

Inc., No. 1:20-cv-03590 (D.D.C. 2025) (FTC monopolization suit filed Dec. 2020, pending); United States v. Google LLC, No. 1:23-cv-00108 (E.D. Va. Nov. 2024) (DOJ advertising technology antitrust suit, liability found Apr. 2025).

24. See Steve Lohr, *The Message for Big Tech in the Google Ruling: Play Nice, but Play On*, N.Y. TIMES (Sept. 3, 2025), <https://www.nytimes.com/2025/09/03/technology/google-ruling-antitrust.html> [<https://perma.cc/344Q-BXQ3>].

25. See, e.g., Dara Kerr et al., *'Slap on the Wrist': Critics Decry Weak Penalties on Google After Landmark Monopoly Trial*, GUARDIAN (Sept. 3, 2025), <https://www.theguardian.com/technology/2025/sep/03/google-monopoly-case-ruling> [<https://perma.cc/A2TG-853K>].

26. See *Ohio v. Am. Express Co.*, 585 U.S. 529, 541 (2018).

27. See, e.g., Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preferences for Privacy*, 16 BERKELEY BUS. L.J. 39 (2019); see also *FTC Hearing #6: Privacy, Big Data, and Competition*, FED. TRADE COMM'N (Nov. 6–8, 2018), <https://www.ftc.gov/news-events/events/2018/11/ftc-hearing-6-privacy-big-data-competition> [<https://perma.cc/ME2H-P736>].

28. Of course, where the data collection is not known to the user, as in the privacy cases discussed earlier, avoidance is impossible even if competitive alternatives exist. See *supra* notes 16–21 and accompanying text (discussing FTC data broker enforcement actions).

true when engagement with these firms is necessary to participate in the economy. Journalist Kashmir Hill powerfully documented this phenomenon in her efforts to cut big tech giants out of her life; she found that ordinary participation in modern economic and social life was “impossible” without interacting with them, with a limited exception for Apple.²⁹ And even if people could escape personal interaction with these platforms, they cannot opt out of having location data, search history, or communications metadata collected by choosing a different provider if all providers feed (or are fed by) the same underlying data ecosystem.³⁰

Second, concentration eliminates competitive discipline on data practices. In a competitively functioning market, firms are deterred from misusing consumer data for fear that doing so will drive customers to their rivals. In concentrated markets, this discipline does not operate effectively. Dominant firms can engage in practices that consumers would reject if they had the option to do so, secure in the knowledge that no adequate alternative exists, and therefore consumer rejection is not an option. Concentration may explain why we see so many large firms engaging in privacy violations: doing so is economically efficient, because they can be confident that the market does not provide switching opportunities.³¹

Third, and most importantly for the argument of this Essay, concentration creates catastrophic single points of failure. When data is diffusely distributed across many firms, the compromise, coercion, or misuse of any one firm’s data is contained. When data is concentrated, the compromise of a single firm exposes the entire population. Today, a government that wants detailed behavioral profiles of its population needs only to approach a handful of dominant firms. Concentration creates, in effect, a convenient surveillance infrastructure for

29. See Kashmir Hill, *I Cut the “Big Five” Tech Giants from My Life. It Was Hell*, GIZMODO (Feb. 7, 2019), <https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194> [<https://perma.cc/K5LD-D5CB>]; see also Kashmir Hill, *I Tried to Block Amazon from My Life. It Was Impossible*, GIZMODO (Jan. 22, 2019), <https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336> [<https://perma.cc/6A6Y-SZVM>].

30. See *infra* Section III.B.

31. See Deepak Gupta, *Billions in Fines, Barely a Bruise: What Big Tech Penalties Really Mean for Your Privacy*, SEC. BOULEVARD (July 4, 2026), <https://securityboulevard.com/2026/07/billions-in-fines-barely-a-bruise-what-big-tech-penalties-really-mean-for-your-privacy/> [<https://perma.cc/4DLG-NF4X>].

any actor with the willingness and ability to exploit it. Concentration converts data from a distributed risk into a systemic one.

III. EXECUTIVE POWER

A. *Expansion of the Power of the President over Government Institutions*

In his second term, President Trump has taken action across multiple vectors that consolidate power in himself and his office, at the expense of other branches of government: Congress, the judiciary, and independent watchdogs.

He has claimed power to alter via executive order the constitutional guarantee of birthright citizenship, an effort rejected by the Supreme Court.³² The Court has also struck down his attempts to unilaterally issue tariffs under the International Emergency Economic Powers Act (“IEEPA”).³³ There are legal challenges pending to his efforts to dismantle federal agencies established by Congress,³⁴ raze the federal workforce and the statutory protections attached to civil servant positions,³⁵ and overhaul the immigration system,³⁶ among many other executive actions. Of particular personal interest, the President challenged longstanding Supreme Court precedent in order to fire Senate-

32. See *Trump v. Barbara*, 146 S. Ct. 2438 (2026). Multiple district courts issued nationwide injunctions against the executive order before the Supreme Court granted certiorari. *Id.* Ultimately, a divided Supreme Court struck down the executive order on both constitutional and statutory grounds. *Id.*

33. See *Learning Res., Inc. v. Trump*, 146 S. Ct. 628 (2025) (holding tariffs imposed under International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1707, exceeded scope of statute).

34. See, e.g., *Nat’l Treasury Emps. Union v. Vought*, 774 F. Supp. 3d 1 (D.D.C. 2025) (challenging Consumer Financial Protection Bureau operational shutdown).

35. See, e.g., *Am. Fed’n of Gov’t Emps. v. Trump*, No. 3:25-cv-03698 (N.D. Cal. 2025) (challenging Department of Government Efficiency (“DOGE”) – directed cuts). Civil service protections are established by statute in the Civil Service Reform Act of 1978, 5 U.S.C. §§ 7511–7514.

36. See, e.g., *Trump v. Illinois*, 146 S. Ct. 432 (2025) (rejecting Administration’s application for stay of lower court decision blocking deployment of National Guard troops to Chicago to aid immigration enforcement); *Amica Ctr. for Immigrant Rts. v. Exec. Off. for Immigr. Rev.*, 822 F. Supp. 3d 119 (D.D.C. 2026).

confirmed members of independent boards and commissions.³⁷ The Court ultimately overturned the precedent in *Humphrey's Executor*, allowing my own removal from the FTC to stand,³⁸ and that new precedent has been applied to other independent boards and commissions.³⁹ Thus far, the only excepted agency has been the Federal Reserve.⁴⁰

In all of these cases, the President is not only taking power for himself; he is taking it from Congress through assertions that statutory limitations on executive power are anathema to the Constitution. But providing limitations on executive power is precisely what the Constitution is designed to do; the Take Care Clause says that the President shall "take care that the laws be faithfully executed,"⁴¹ not take care to ensure he can achieve his preferred policy outcomes by any means necessary. The laws he must faithfully execute are, under our Constitution, written and passed by Congress; to the extent that the President asserts the power to ignore or rewrite those laws on his own, he is taking the power of Congress under Article I to pass and the judiciary under Article III to interpret those laws. In the cases in which the President ultimately prevailed, such as my own, it is because the judiciary acceded to this transfer of power.

37. See *Trump v. Slaughter*, 146 S. Ct. 2883 (2026); see also *Trump v. Wilcox*, 145 S. Ct. 1415 (2025) (Supreme Court stay permitting removal of National Labor Relations Board member Gwynne Wilcox and Merit Systems Protection Board member Cathy Harris pending merits review); *Trump v. Boyle*, 145 S. Ct. 2653 (2025) (Supreme Court stay permitting removal of Consumer Product Safety Commissioners). All three cases involve the application of *Humphrey's Executor v. United States*, 295 U.S. 602 (1935), to specific independent agencies. In addition, the Court considered on procedural grounds President Trump's attempted removal of Federal Reserve Board Governor Lisa Cook, purportedly for cause. *Trump v. Cook*, 146 S. Ct. 2234 (2026). And lower courts have been considering the President's attempt to remove the Democratic members of the Privacy and Civil Liberties Oversight Board. See *LeBlanc v. U.S. Priv. & Civ. Liberties Oversight Bd.*, 784 F. Supp. 3d 1 (D.D.C. 2025).

38. See *Slaughter*, 146 S. Ct. at 2883.

39. See, e.g., *Harris v. Bessent*, 160 F.4th 1235 (D.C. Cir. 2025) (upholding district court decision permitting removal of Merit Systems Protection Board Member Cathy Harris), *cert. denied*, No. 25-1110 (U.S. June 30, 2026).

40. See *Cook*, 146 S. Ct. at 2234. Courts have not yet resolved how to treat the Copyright Office; the DC Circuit blocked the removal of the Director of Copyrights, and even after resolving *Trump v. Slaughter*, the Supreme Court declined to review the DC Circuit decision. See *Perlmutter v. Blanche*, No. 25-5285, 2025 WL 2627965 (D.C. Cir. Oct. 1, 2025), *cert. denied*, No. 25A478 (US Oct. 27, 2025).

41. See U.S. CONST. art. II, § 3.

B. Executive Power and Data-Driven Markets

The example of the President ignoring statutory removal protections in order to fire commissioners at independent boards and commissions is of particular relevance in this conversation not only because it is personal to me, but also because independent agencies are tasked with privacy oversight. Two of the agencies from which he has removed Commissioners—my own, the FTC, and the Privacy and Civil Liberties Oversight Board (“PCLOB”)—are charged with regulating privacy. The FTC focuses on commercial actors,⁴² and the PCLOB oversees government actors.⁴³ The FTC also enforces competition laws.⁴⁴

The Federal Trade Commission was established in 1914 as a bipartisan, multi-member body with the authority to prevent unfair methods of competition and, over time, unfair or deceptive acts and practices, including in the handling of consumer data.⁴⁵ By statute, its Commissioners can be removed only in the case of “inefficiency, neglect of duty, or malfeasance in office.”⁴⁶ The FTC is not the only agency that Congress designed to apply expert, consistent, politically insulated oversight to markets that require it; there are over two dozen “independent” agencies,⁴⁷ including the Federal Reserve.⁴⁸ The independence of these agencies is not incidental to their function; it is a core part of their institutional design by Congress.⁴⁹

For privacy regulation in particular, independence is essential in several respects. The companies whose privacy practices are most problematic are often among the most powerful and politically connected actors in the economy. Sustained

42. 15 U.S.C. § 45(a)(1) (declaring “unfair or deceptive acts or practices in or affecting commerce” unlawful).

43. 42 U.S.C. § 2000ee.

44. 15 U.S.C. § 45(a)(1) (declaring “[u]nfair methods of competition in or affecting commerce” unlawful).

45. See FED. TRADE COMM’N, REPORT TO CONGRESS ON PRIVACY AND DATA SECURITY (Sept. 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf [<https://perma.cc/R5B6-HZU4>].

46. See 15 U.S.C. § 41.

47. See *Seila Law LLC v. CFPB*, 591 U.S. 197, 230 (2020).

48. See 12 U.S.C. § 242 (providing that members of Federal Reserve Board of Governors may be removed only “for cause”).

49. For a discussion of the history of independent agencies, see generally Brief for Respondent at 12–23, *Trump v. Slaughter*, 146 S. Ct. 2883 (2026) (No. 25-332).

enforcement against those actors requires the ability to resist pressure from both the companies themselves and from elected officials who may benefit from their support. That is why it has made sense that privacy oversight in the United States has historically lived in agencies, the FTC and the PCLOB, that were designed with for-cause removal protections to insulate independent agency commissioners from dismissal at the President's pleasure, in order to ensure that decisions are made on the merits, not in response to political calculations.⁵⁰

Now that the President can remove FTC commissioners at will, the privacy implications are severe. First, enforcement against politically connected tech companies will become a political calculation. A commissioner who votes to pursue enforcement against a company whose executives are major political donors, or who provides services valuable to the White House, now does so at personal professional risk. The chilling effect on enforcement will be profound and need not be explicit; the mere possibility of removal for inconvenient decisions would suffice to distort institutional judgment, which in turn undermines the credibility of all agency actions.

Consider two contrasting examples: In 2019, the FTC settled with Facebook for five billion dollars over privacy violations.⁵¹ Though Commissioner Chopra and I dissented, believing the settlement to be insufficient to deter future violations,⁵² the public could trust the process was legitimate; our dissents would have exposed any corruption. Compare that to the 2025 Amazon settlement, inked after minority Commissioners had been

50. See *Slaughter*, 146 S. Ct. at 2883 (Sotomayor, J., dissenting) ("Since the founding, Congress has created agencies that in various ways have embodied th[e] goal of independence. Over the last 140 years especially, the political branches have done so by establishing agencies like the Federal Trade Commission (FTC): bipartisan, multimember bodies with 'for-cause' removal protections. This structure allows the agencies to address complex problems while enjoying some independence from Presidential removal and thus absolute partisan control.").

51. See *United States v. Facebook, Inc.*, No. 19-cv-2184, ECF No. 38-1 (D.D.C. May 31, 2023) (imposing five billion dollar civil penalty for violations of 2012 FTC order); see also Facebook Press Release, *supra* note 6.

52. *Slaughter Facebook Dissent*, *supra* note 6; see Dissenting Statement of Commissioner Rohit Chopra Regarding the Matter of Facebook, Inc. (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [<https://perma.cc/M6TR-UADE>].

removed from the FTC.⁵³ FTC staff had won key pretrial motions, but the agency settled for US\$2.5 billion—a fraction of Amazon’s potential penalty exposure, with no admission of liability—in the wake of Amazon donating millions to Trump’s inauguration,⁵⁴ contributing to his White House renovation,⁵⁵ and paying forty million dollars to the First Lady.⁵⁶ Was this a fair result for consumers, or a political favor? I genuinely don’t know—I was locked out of the process. Without independent commissioners, the public has no way to know if powerful actors are escaping accountability due to political favoritism.⁵⁷

Second, the FTC’s own data holdings would become vulnerable to access by other parts of the federal government, notwithstanding statutory provisions that prevent such access.⁵⁸ The Commission collects and retains extraordinarily sensitive confidential business information from the American public and

53. See Press Release, Fed. Trade Comm’n, FTC Secures Historic \$2.5 Billion Settlement Against Amazon (Sept. 25, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon> [<https://perma.cc/UQF6-MLGN>].

54. See Rebecca Falconer, *Amazon Gives \$1M to 2025 Inaugural Fund in Latest Big Tech Gift for Trump*, AXIOS (Dec. 12, 2024), <https://www.axios.com/2024/12/13/amazon-trump-inauguration-1-million> [<https://perma.cc/HM4H-CEPF>].

55. See Liz Landers & Joshua Barajas, *Who’s Paying for Trump’s \$300 Million Ballroom*, PBS NEWS (Oct. 23, 2025), <https://www.pbs.org/newshour/politics/whos-paying-for-trumps-300-million-ballroom> [<https://perma.cc/SV9J-RMD4>].

56. See Tamara Keith, *Big-Budget Melania Trump Documentary Premieres with Splashy Rollout*, NAT’L PUB. RADIO (Jan. 29, 2026), <https://www.npr.org/2026/01/29/nx-s1-5689040/big-budget-melania-trump-documentary-premieres-with-splashy-rollout> [<https://perma.cc/TZD2-BP7D>].

57. For a more detailed discussion of the implications of the evisceration of agency independence and for-cause removal protections, see Rebecca Kelly Slaughter, *What Humphrey’s Legacy Protects*, REGUL. REV. (Mar. 2, 2026), <https://www.theregreview.org/2026/03/02/slaughter-what-humphreys-legacy-protects/> [<https://perma.cc/U73L-WP3W>].

58. Disclosure of nonpublic information held by the FTC is a crime. See 15 U.S.C. § 50. An entire section of the FTC Act, 15 U.S.C. § 57b-2, titled “Confidentiality,” governs the confidentiality of information received by the agency. This section provides particular confidentiality rules for material received “pursuant to compulsory process in an investigation.” 15 U.S.C. § 57b-2(b)(3)(C) (“[N]o documentary material, tangible things, reports or answers to questions, and transcripts of oral testimony shall be available for examination by any individual other than a duly authorized officer or employee of the Commission without the consent of the person who produced the material, things, or transcripts.”). Additional specific provisions protect trade secrets or confidential commercial information the Commission obtains from any person, 15 U.S.C. § 46(f), and premerger notification filings made pursuant to the Hart-Scott-Rodino Act. 15 U.S.C. § 18a(h).

the business community: consumer complaints, merger filings, responses to civil investigative demands, consent order compliance materials. I was deeply concerned about what would happen if the Department of Government Efficiency (“DOGE”) members accessed this data. I was removed before DOGE arrived at the FTC, but, based on the information publicly available about the role of DOGE at other agencies, my concerns were not misplaced. For example, in March 2026, it became public that a whistleblower alleged that a DOGE team member deployed to the Social Security Administration had extracted sensitive personal data on millions of Americans.⁵⁹ If the President wants to get and use or share data held by the FTC, at-will Commissioners are largely powerless to stop him from doing so.

C. Executive Power over Private Actors

In addition to his rejection of legal limitations on his power over government actors, President Trump has asserted extraordinary power over private corporations as well, demonstrating himself both willing to use instruments of government leverage and vindictive in doing so. For example, he has bullied law firms⁶⁰ and universities⁶¹ to adopt his preferred personnel policies and business practices. In some cases, these

59. See Meryl Kornfeld et al., *Whistleblower Claims Ex-DOGE Member Says He Took Social Security Data to New Job*, WASH. POST (Mar. 10, 2026), <https://www.washingtonpost.com/politics/2026/03/10/social-security-data-breach-doge-2/> [https://perma.cc/DZG4-DLRA].

60. See, e.g., Exec. Order No. 14230, 90 Fed. Reg. 11781 (Mar. 11, 2025); see also Michael S. Schmidt et al., *Law Firms Made Deals with Trump. Now He Wants More from Them*, N.Y. TIMES (Apr. 16, 2025), <https://www.nytimes.com/2025/04/16/us/politics/law-firms-deals-trump.html> [https://perma.cc/8TFD-9B6N]. The executive orders directed federal agencies to revoke security clearances, deny access to federal buildings, and terminate federal contracts with named law firms. See Exec. Order No. 14230, 90 Fed. Reg. at 11781.

61. See Michael C. Bender et al., *Investigations and a Billion-Dollar ‘Shakedown’: How Trump Targeted Higher Education*, N.Y. TIMES (Jan. 21, 2026), <https://www.nytimes.com/2026/01/21/us/politics/trump-higher-education-2025.html> [https://perma.cc/5F4R-LYRD]. The administration targeted at least seventy-five universities, threatening to terminate hundreds of millions of dollars in federal research grants and contracts unless universities altered admissions, hiring, and campus speech policies. See *id.*

institutions caved to the pressure and accepted his terms; those that have pushed back legally have been successful thus far.⁶²

The President and his proxies at formerly independent agencies have also tried to control speech by private corporations. Upset at what he perceived to be negative coverage of himself and his administration, the President lashed out at the networks ABC and CBS. In addition to filing personal lawsuits against them demanding monetary damages, which both companies settled for sixteen million dollars each after the President was reelected,⁶³ the President suggested that Federal Communications Commission ("FCC") Chairman Brendan Carr revoke broadcast licenses.⁶⁴ While Paramount, the parent company of CBS, was seeking FCC approval for its merger with Skydance, it announced it was canceling Stephen Colbert's late-night comedy show, which had consistently poked fun at the President.⁶⁵ When Jimmy Kimmel, on his own comedy show that airs on ABC, sparked the ire of conservatives for speculation about Charlie Kirk's death, Chairman Carr suggested that ABC might lose its broadcast license.⁶⁶ Local affiliates at stations owned by Nexstar and Sinclair took Kimmel off the air, but were met with outrage by viewers and swiftly reversed the decision.⁶⁷ But the episode revealed how willing and able the

62. See, e.g., Michael S. Schmidt et al., *Trump Administration, in Reversal, Tries to Continue Fight Against Law Firms*, N.Y. TIMES (Mar. 3, 2026), <https://www.nytimes.com/2026/03/03/us/politics/trump-law-firm-orders-reversal.html> [<https://perma.cc/2MFL-4P65>]; see also Michael C. Bender et al., *Trump Is Said to Have Dropped Demand for Cash from Harvard*, N.Y. TIMES (Feb. 2, 2026), <https://www.nytimes.com/2026/02/02/us/politics/trump-harvard-payment.html> [<https://perma.cc/9V4K-W8BM>].

63. See Tatiana Siegel et al., *Disney's Settlement with Donald Trump: Bob Iger's \$16 Million Decision, Fear at ABC News and Questions About George Stephanopoulos' Future*, VARIETY (Dec. 18, 2024), <https://variety.com/2024/tv/news/abc-news-trump-settlement-backlash-george-stephanopoulos-1236253269/> [<https://perma.cc/A9XK-K4CW>]; see also David Bauder, *Paramount Will Pay \$16 Million in Settlement with Trump over '60 Minutes' Interview*, ASSOCIATED PRESS (July 2, 2025), <https://www.ap.org/news-highlights/spotlights/2025/paramount-will-pay-16-million-in-settlement-with-trump-over-60-minutes-interview/> [<https://perma.cc/4K4G-93L5>].

64. See David Folkenflik, *Jimmy Kimmel's Suspension Shows Power of FCC's Brendan Carr*, NAT'L PUB. RADIO (Sept. 19, 2025), <https://www.npr.org/2025/09/19/nx-s1-5546764/fcc-brendan-carr-kimmel-trump-free-speech> [<https://perma.cc/F6EM-CMFJ>].

65. See Mandalit del Barco, *CBS Will End 'The Late Show with Stephen Colbert' Next Year*, NAT'L PUB. RADIO (July 17, 2025), <https://www.npr.org/2025/07/17/nx-s1-5471581/cbs-stephen-colbert-late-show> [<https://perma.cc/9APU-NFX4>].

66. See Folkenflik, *supra* note 64.

67. See *id.*

historically independent agency was to wield power to punish President Trump's perceived enemies and reward his allies.

My own former agency, the FTC, has entered the speech-police fray on behalf of President Trump and his allies, against conservative bugaboos. In May 2025, after Commissioner Bedoya and I were removed, the FTC issued a civil investigative demand ("CID") to Media Matters, a nonprofit media company, seeking information purportedly to support an investigation into an advertiser boycott of X.⁶⁸ Media Matters had published an article in 2023 reporting that, since Elon Musk had acquired the social media platform formerly known as Twitter and changed its content moderation policies, advertisements on the platform were now appearing next to offensive Nazi posts.⁶⁹ This article triggered many advertisers to withdraw from the platform and enraged Mr. Musk, a close ally of President Trump, who vowed "thermonuclear" revenge.⁷⁰ The FTC's investigation was not the only one to target Media Matters; state attorneys general had sued as well (and been enjoined).⁷¹ But the FTC's investigation represented a dramatic break from Commission practice, and also violated the Constitution. The district court hearing Media Matters' suit to enjoin the CID held that "Media Matters engaged in quintessential First Amendment activity when it published an online article criticizing Mr. Musk and X. And the Court finds that the FTC's expansive CID is a retaliatory act."⁷²

And finally, the President has induced contributions, both direct and indirect, from private actors seeking to curry favor with the administration. According to an analysis by the Brennan Center, President Trump's second inauguration drew more contributions of at least one million dollars than any previous inauguration, nearly three times the previous record, which was

68. See *Media Matters for Am. v. FTC*, 805 F. Supp. 3d 105 (D.D.C. 2025).

69. See Eric Hananoki, *As Musk Endorses Antisemitic Conspiracy Theory, X Has Been Placing Ads for Apple, Bravo, IBM, Oracle, and Xfinity Next to Pro-Nazi Content*, MEDIA MATTERS FOR AM. (Nov. 16, 2023), <https://www.mediamatters.org/twitter/musk-endorse-antisemitic-conspiracy-theory-x-has-been-placing-ads-apple-bravo-ibm-oracle> [https://perma.cc/32ZK-GX2T].

70. See *Media Matters for Am. v. FTC*, 805 F. Supp. 3d at 113.

71. See *Media Matters for Am. v. Paxton*, 138 F.4th 563 (D.C. Cir. 2025); see also *Media Matters for Am. v. Paxton*, No. 1:24-cv-00147 (D.D.C. 2024).

72. See *Media Matters for Am. v. FTC*, 805 F. Supp. 3d at 112.

set at President Trump's first inauguration.⁷³ The industry that gave the most was tech, accounting for over US\$44.6 million out of the total US\$245 million the inaugural committee collected.⁷⁴ When he decided he wanted to tear down the historic East Wing of the White House to construct an oversized ballroom—a project that was not approved or authorized by Congress—President Trump solicited over US\$300 million worth of private donations from companies with an interest in the federal government, as contractors, regulated entities, or both.⁷⁵ The collection of companies includes most of those same tech giants that control sensitive personal data on almost all Americans: Microsoft, Google, Palantir, and Amazon.⁷⁶

Taken together, the picture is clear: President Trump is exercising direct control over parts of government designed to be removed from political interference, and over private actors who incur his ire. He is using this control to exact a campaign of retribution and domination against those who have offended him or his political allies. And right in the crosshairs are some of the companies that not only control comprehensive data about the American people, but whose business fortunes depend on whether and to what extent they are treated favorably by the federal government.

IV. THE THREAT MULTIPLIER: WHEN THE TWO PROBLEMS COLLIDE

A. *The Architecture of Coercion*

The problems described in the preceding two Sections—unchecked data concentration and unbalanced executive power—are each serious in their own right. But in combination, they present a holistic problem that is greater than the sum of

73. See Anna Massoglia, *Million-Dollar Donors Flooded Trump's Second Inauguration*, BRENNAN CTR. (July 1, 2025), <https://www.brennancenter.org/our-work/research-reports/million-dollar-donors-flooded-trumps-second-inauguration> [<https://perma.cc/LJ7Q-UHR4>].

74. See *id.*

75. See Laura Doan & Julia Ingram, *What Donors to Trump's White House Ballroom Stand to Gain from the Federal Government*, CBS NEWS (Oct. 25, 2025), <https://www.cbsnews.com/news/trump-ballroom-donors-white-house-stand-to-gain/> [<https://perma.cc/C6R3-LPV2>].

76. See *id.*

its parts. When a small number of corporations whose business interests depend on the federal government hold comprehensive data on the entire population, and when the government can and will direct or coerce those corporations without meaningful independent regulatory check, the result is a qualitatively new form of surveillance power that has no precedent in American history.

Consider what this combination makes possible. A President who controls independent agencies and has political relationships with the dominant tech platforms holds, in effect, the ability to access detailed behavioral profiles of anyone in the country, including their location history, communications metadata, financial transactions, health decisions, political associations, and social networks. It can do so without a warrant, without judicial oversight, and without the independent regulatory check that Congress specifically created to prevent this kind of accumulation of power. The President need not issue a formal order compelling disclosure. The implicit leverage created by the combination of regulatory authority and political alliance is itself sufficient. Companies that understand that their regulatory fate depends on their political relationships with the White House have strong incentives to be accommodating.

When I came up with the topic of this Essay in the fall of 2025, this risk was arguably hypothetical; it no longer is. By the time I delivered the talk in March, a very public battle had erupted between the Department of Defense (“DOD”) and the company Anthropic,⁷⁷ whose investors include Microsoft, Amazon, and Google.⁷⁸ One of two key sticking points between the parties was that Anthropic wanted legal protections in its contract with DOD that would prohibit the use of its technology for mass surveillance

77. See Michael Kaplan et al., *Internal Pentagon Memo Orders Military Commanders to Remove Anthropic AI Technology from Key Systems*, CBS NEWS (Mar. 10, 2026), <https://www.cbsnews.com/news/pentagon-ai-anthropic-memo-remove-from-key-systems/> [<https://perma.cc/W73U-XGHD>].

78. See Cade Metz, *Anthropic Pushes Its Valuation to \$380 Billion with New Funding Round*, N.Y. TIMES (Feb. 12, 2026), <https://www.nytimes.com/2026/02/12/technology/anthropic-valuation-380-billion-funding.html> [<https://perma.cc/L5UT-XGYL>]; see also FED. TRADE COMM’N, PARTNERSHIP BETWEEN CLOUD SERVICE PROVIDERS AND AI DEVELOPERS: FTC STAFF REPORT ON AI PARTNERSHIP & INVESTMENT 6(B) STUDY (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246201_aipartnerships6breport_redacted_0.pdf [<https://perma.cc/NUP9-E6QK>].

of the American people.⁷⁹ The administration would not agree to Anthropic's terms, which is of course its right; the government has no obligation to contract with any particular private business. However, the government's unwillingness to explicitly exclude mass surveillance from its permitted uses of Anthropic's tools suggests that the administration is very much interested in using the data held and tools created by large tech companies to access private information about Americans.

When Anthropic did not agree to DOD's terms, the administration terminated the contract and also designated Anthropic a supply chain risk.⁸⁰ The President claimed that this designation would not only cut Anthropic off from DOD work, but would also prohibit any business with government contracts from doing business with Anthropic, an effective corporate death sentence.⁸¹ And, according to the lawsuit Anthropic filed against DOD, the intimidation tactics are working,⁸² whether or not they are legal.⁸³ OpenAI, which also counts Microsoft as a major investor, quickly jumped in to take Anthropic's spot. There are competing views about whether OpenAI agreed to facilitate surveillance that Anthropic rejected.⁸⁴

79. See Sheera Frenkel et al., *How Talks Between Anthropic and the Defense Dept. Fell Apart*, N.Y. TIMES (Mar. 1, 2026), <https://www.nytimes.com/2026/03/01/technology/anthropic-defense-dept-openai-talks.html> [<https://perma.cc/HS6D-5WTB>]. A central dispute in the contract negotiation was Anthropic's insistence on explicit contractual prohibitions against the use of its technology for mass surveillance of the American public, which the administration declined to accept. *See id.*

80. See Kaplan et al., *supra* note 77; see also Cade Metz et al., *Pentagon Officially Notifies Anthropic It Is a 'Supply Chain Risk'*, N.Y. TIMES (Mar. 5, 2026), <https://www.nytimes.com/2026/03/05/technology/anthropic-supply-chain-risk-defense-department.html> [<https://perma.cc/H9GN-265G>].

81. See Donald Trump (@realDonaldTrump), TRUTH SOCIAL (Feb. 27, 2026, at 03:47 ET), <https://truthsocial.com/@realDonaldTrump/posts/116144552969293195> [<https://perma.cc/TKP8-96WL>].

82. See Jack Queen, *Anthropic Has Strong Case against Pentagon Blacklisting, Legal Experts Say*, REUTERS (Mar. 11, 2026), <https://www.reuters.com/legal/legalindustry/anthropic-has-strong-case-against-pentagon-blacklisting-legal-experts-say-2026-03-11/> [<https://perma.cc/8655-AQEX>].

83. See Paresh Dave, *Anthropic Claims Pentagon Feud Could Cost It Billions*, WIRED (Mar. 9, 2026), <https://www.wired.com/story/anthropic-claims-business-is-in-peril-due-to-supply-chain-risk-designation/> [<https://perma.cc/XJ4D-2DP6>].

84. See Cade Metz, *A Guide to the Pentagon's Dance with Anthropic and OpenAI*, N.Y. TIMES (Mar. 7, 2026), <https://www.nytimes.com/2026/03/07/technology/anthropic-openai-pentagon-dario-amodei-sam-altman.html> [<https://perma.cc/4JWT-AXZB>].

This real-time example illustrates how the combination of the President's strong-arm tactics and the power of large tech companies works hand in hand to create substantial privacy risks. The message to every other company is unsubtle: Agree to our terms (including on surveillance), or we will punish you.

B. Government-as-Purchaser

There is a more direct version of this problem that does not require even the implicit coercion of political relationships: the government can simply purchase the data it wants to access. If data is for sale on a commercial market, the government can buy it. The government has long been a significant purchaser of commercially available data from private brokers; direct purchase can allow the government to circumvent the procedural and substantive Fourth Amendment protections that would otherwise limit government surveillance and trigger judicial oversight.

The Gravy Analytics and Venntel enforcement actions that I joined in December 2024 directly illustrated this problem.⁸⁵ Venntel, the subsidiary whose practices we found most troubling, sold precise geolocation data derived from mobile devices to federal agencies, including the Department of Homeland Security.⁸⁶ The legal theory underlying this practice, which Commissioner Bedoya's statement aptly described as the porous line between government and private surveillance, is that data voluntarily provided to a private company loses its Fourth Amendment protection, and may therefore be purchased by the government without a warrant.⁸⁷ This enables the government to acquire detailed surveillance data on the entire population at the cost of a commercial data subscription.

When the agencies charged with regulating data broker practices are subject to direct presidential control, this loophole becomes a structural void. A White House that wants access to location histories, behavioral profiles, or communications patterns can direct a politically controlled FTC to abandon

85. See Gravy Analytics Press Release, *supra* note 16.

86. See Bedoya Statement, *supra* note 17 (describing how Venntel's customers included federal agencies such as the Department of Homeland Security, the Drug Enforcement Administration, the FBI, and the IRS).

87. See *id.*

enforcement against the brokers who sell such data to the government, or can simply decline to investigate. The regulatory check against government data purchases becomes an executive permission slip.

C. Tech-Titan-as-Political-Ally

The political alignment between dominant technology companies and the current administration represents a further dimension of this problem. Over the last decade, the dominant platforms were cast as adversaries of the political right, subject to accusations of politically motivated content moderation.⁸⁸ By early 2025, several of those same companies had realigned dramatically: their executives were present at President Trump's inauguration;⁸⁹ their firms donated to the President's pet projects;⁹⁰ and their regulatory concerns were promptly addressed.⁹¹

The structural implications of this realignment for privacy are significant. When the firms that hold the most comprehensive data on the American population are also major political allies of the administration, the distinction between government surveillance and corporate surveillance begins to dissolve. A government that cannot directly compel disclosure without legal process can achieve equivalent results by cultivating relationships with firms that hold the relevant data and have strong incentives to be accommodating. The formal

88. See, e.g., Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Senate Commerce Investigation Reveals How Big Tech Weaponizes Terms of Service to Silence the Right (Apr. 24, 2024), <https://www.commerce.senate.gov/press/rep/release/senate-commerce-investigation-reveals-how-big-tech-weaponizes-terms-of-service-to-silence-the-right-2024-4/> [<https://perma.cc/L6DU-BSMJ>].

89. See Ali Swenson, *Trump, a Populist President, Is Flanked by Tech Billionaires at His Inauguration*, ASSOCIATED PRESS (Jan. 20, 2025), <https://apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d941d62cebc3074267ecd> [<https://perma.cc/YU8F-4KST>] (describing prominent front-row seating of the chief executives of Meta, Amazon, Google, and other major technology companies at President Trump's inauguration ceremony). Elon Musk, whose companies include xAI and X (formerly Twitter), stood immediately behind Trump as he took the oath of office. See *id.*

90. See Landers & Barajas, *supra* note 55.

91. See, e.g., Jennifer Elias, *Trump Signs Executive Order for Single National AI Regulation Standard, Limiting Power of States*, CNBC (Dec. 11, 2025), <https://www.cnbc.com/2025/12/11/trump-signs-executive-order-for-single-national-ai-regulation-framework.html> [<https://perma.cc/B95M-86DD>].

boundary between public and private surveillance becomes a permeable membrane.

This is why the competition-privacy nexus matters so much. In a healthy competitive market with effective privacy laws, no single company holds data on everyone. In a concentrated market, the accommodation of one or two dominant firms can provide access to data on the entire population. As a result, market concentration is not merely a competition problem, it is a national security and civil liberties problem.

D. Precedent and Pattern: Historical Lessons

The convergence of government surveillance power and commercial data infrastructure is not wholly unprecedented. The Church Committee's investigations in 1975 and 1976 documented the government intelligence ecosystem that evolved in the period after World War II.⁹² The Committee concluded that "the operation of an extensive and necessarily secret intelligence system places severe strains on the nation's constitutional government."⁹³ Those revelations produced significant legislative reform, including the Foreign Intelligence Surveillance Act ("FISA"), premised on the conviction that government surveillance power, in the absence of meaningful oversight, would inevitably be turned against political opponents and dissenters.⁹⁴

The post-September 11th expansion of surveillance authorities raised similar concerns in a new technological context. The National Security Agency's ("NSA") bulk collection programs revealed by Edward Snowden in 2013⁹⁵ demonstrated that the

92. See Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, S. Rep. No. 94-755 (1976).

93. See *id.* bk. I, at 425.

94. See Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.). Congress enacted FISA in direct response to the Church Committee's findings, establishing a specialized court to review government applications for surveillance warrants targeting foreign intelligence, and codifying limitations on intelligence collection within the United States that had previously been absent from law. See *id.*

95. See Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), <https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html> [https://perma.cc/2B5Q-

combination of legal authority, however dubiously construed,⁹⁶ and technical capability could produce surveillance infrastructure of truly staggering scope. The legal reforms that followed, including the USA FREEDOM Act⁹⁷ and the 9/11 Commission Act, which established the PCLOB as an independent referee,⁹⁸ reflected a recognition that the earlier framework had failed.

What makes the current moment different, and in important respects more dangerous, is the combination of three factors that were not present, or were present only in weaker form, in these earlier episodes. First, the private sector data holdings now available to a government willing to exploit them are incomparably more comprehensive than anything available to prior generations of intelligence gathering. Second, the legal checks—Fourth Amendment doctrine, FISA oversight, the Privacy Act—were designed for a world in which government and corporate surveillance were separate domains. They have not kept pace with the public-private fusion I have described. And third, the independence of the institutional check on corporate abuses, the FTC, has been eliminated.

UJFV]; see also Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [<https://perma.cc/XGB8-ENYQ>]. The disclosures revealed bulk collection programs under Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (expired 2020), and Section 702 of FISA, codified at 50 U.S.C. § 1881a.

96. The bulk surveillance programs revealed by Snowden were later held to be illegal. See Charlie Savage & Jonathan Weisman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. TIMES (May 7, 2015), <https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html> [<https://perma.cc/8K6S-KGMU>].

97. See Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 50 U.S.C.) (ending National Security Agency (“NSA”) bulk telephone metadata collection and strengthening oversight mechanisms).

98. See *History and Mission*, U.S. PRIV. & CIV. LIBERTIES OVERSIGHT BD., <https://www.pclob.gov/About/HistoryMission> [<https://perma.cc/7DVC-8C5J>] (last visited Sept. 13, 2026).

V. THE INTERNATIONAL DIMENSION: AMERICAN DATA POWER
HAS NO BORDERS

A. US Platforms Hold the World's Data

The risks described in the preceding sections are not confined to American citizens. The dominant data-holding entities at the center of this discussion are overwhelmingly American companies: Google, Meta, Amazon, Apple, Microsoft, and the data-broker ecosystem that feeds off their digital infrastructure. But they operate internationally, and their data holdings are not bounded by citizenship or geography. They hold health, location, behavioral, and communications data on billions of non-American persons worldwide.⁹⁹ The data of a French journalist, a Turkish opposition politician, a Brazilian labor organizer, a South Korean student, or a Mexican immigrant in the United States may sit on American servers, subject to American jurisdiction, and, increasingly, to the discretion of an American executive who faces no meaningful independent regulatory check.

This is not theoretical. The FTC's data broker enforcement actions revealed companies that processed location signals from devices around the world, with no geographic filter on the individuals tracked.¹⁰⁰ The Commission's 2024 report on Social Media and Video Streaming Services documented the vast amount of data collected by the large tech platforms.¹⁰¹ The surveillance advertising architecture is agnostic as to citizenship: A mobile device emitting location signals, generating advertisement impressions, and building a behavioral profile does so regardless of the nationality of its owner. When Gravy Analytics curated seventeen billion location signals daily from around a billion

99. See, e.g., Matilda Davies, *Every Scary Thing Meta Knows About Me — and You*, TIMES (LONDON) (Mar. 16, 2024), <https://www.thetimes.com/uk/healthcare/article/meta-user-data-collection-facebook-instagram-whatsapp-9klqhzlq9> [<https://perma.cc/D5J4-8WWS>] (documenting data collected about UK citizen by Meta).

100. See Gravy Analytics Press Release, *supra* note 16.

101. See FED. TRADE COMM'N, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES (Sept. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf [<https://perma.cc/TU8U-DRDB>].

devices, those devices were not exclusively American.¹⁰² The profiles built on them were not limited to Americans.¹⁰³ The risks created by the absence of adequate regulatory oversight are therefore borne by people everywhere.

B. The Collapse of the United States as a Trusted Data Partner

There are also substantial commercial implications for international businesses. The US approach to data governance has varied significantly from that of its international counterparts, especially Europe.¹⁰⁴ The US model comprises a patchwork of state and federal laws, marked by limits on direct government collection of data, market self-regulation, sectoral statutory protections, and FTC enforcement as the primary backstop against abuse.¹⁰⁵ This model required trading partners to trust that American institutions provided effective protection for their citizens' data when it was transferred to American-based companies.¹⁰⁶ The successive frameworks for transatlantic data flows—Safe Harbor, Privacy Shield, and the current Data Privacy Framework—were premised, at each stage, on the judgment that American law and enforcement provided protection roughly equivalent to the European Union's own standards.¹⁰⁷

That judgment has never been entirely secure. The *Schrems* litigation before the Court of Justice of the European Union

102. See Gravy Analytics Press Release, *supra* note 16. The Mobilewalla complaint in the same enforcement round further documented that location data companies routinely compile profiles on consumers in countries outside the United States. See Complaint, *In re Mobilewalla, Inc.*, FTC File No. 202-3196 (Dec. 3, 2024).

103. See Gravy Analytics Press Release, *supra* note 16.

104. See Elias Aidun, *Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations*, U. CIN. L. REV. BLOG (Mar. 5, 2025), <https://uclawreview.org/2025/03/05/data-privacy-in-the-digital-age-a-comparative-analysis-of-u-s-and-eu-regulations/> [<https://perma.cc/9PJK-DZJA>].

105. *Id.*

106. See, e.g., European Commission Press Release IP/23/3721, Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows (July 9, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 [<https://perma.cc/9F2D-FBKT>] (explaining standards allowing US companies to process Europeans' data, and concluding that "the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies.").

107. *Id.*

("CJEU"), stretching from the first decision in 2015¹⁰⁸ through the *Schrems II* decision in 2020,¹⁰⁹ reflected the fundamental concern, affirmed by the CJEU, that American law did not adequately protect EU data subjects from US government surveillance—specifically, that Section 702 of FISA and Executive Order 12333 authorized collection programs so broad as to render meaningless any commercial privacy protections.¹¹⁰ The Data Privacy Framework negotiated by the Biden administration attempted to address those concerns through new redress mechanisms and collection limitations.¹¹¹ If the United States cannot assure the CJEU that protections against government surveillance are an adequate equivalent to the European protections, the result is that no US company can process any EU citizen's data, and therefore cannot operate in the European Union, an enormously important market economically.

The developments described in this Essay make that risk of a successful adequacy challenge far more acute. Eliminating the PCLOB's independence by firing its commissioners directly affects the credibility of any independent oversight of

108. Case C-362/14, *Schrems v. Data Prot. Comm'r* (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015).

109. Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd.* (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

110. The succession of transatlantic data transfer frameworks reflects repeated findings that US law failed to provide adequate protection for EU data subjects. The Safe Harbor Framework was invalidated by the Court of Justice of the European Union ("CJEU") in 2015 and then replaced by the Privacy Shield. *See* Case C-362/14, *Schrems v. Data Prot. Comm'r* (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015); *Update on the US-EU Safe Harbor Framework*, FED. TRADE COMM'N, <https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework> [<https://perma.cc/5PJC-4KM4>] (last visited Sept. 13, 2026) ("On October 6, 2015, the European Court of Justice issued a judgment declaring invalid the European Commission's July 26, 2000, decision on the legal adequacy of the US-EU Safe Harbor Framework. On July 12, 2016, the European Commission issued an adequacy decision on the EU-US Privacy Shield Framework. This new Framework, which replaces the Safe Harbor program, provides a legal mechanism for companies to transfer personal data from the EU to the United States."). Privacy Shield, in turn, was later invalidated by the CJEU, in a case known as *Schrems II*. *See* Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd.* (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020). In both *Schrems I* and *Schrems II*, the basis for the invalidation was that US national security access undermined the framework's adequacy commitments. *See id.*; *Schrems I*, ECLI:EU:C:2015:650.

111. *See* Commission Implementing Decision 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118; *see also* Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

government surveillance. And eliminating the independence of the FTC compounds that credibility hit by taking out the watchdogs of commercial surveillance. The viability of the United States as a trusted data partner depends on American regulatory institutions functioning as Congress designed them: independent, expert, bipartisan bodies that enforce the law without regard to the political fortunes of the companies they regulate or the administrations they serve. That credibility collapses when commissioners are fired for political reasons, when enforcement priorities are subject to White House direction, and when the largest data holders are cultivated as political allies. Our European partners can hardly be faulted for concluding that American adequacy commitments cannot be trusted when the independence of the institutions making those commitments has been eliminated.

Indeed, the second-guessing of adequacy began immediately after *Trump v. Slaughter*. The organization noyb (short for “none of your business”), whose Honorary Chair is activist Max Schrems, immediately called on the European Commission to rescind its adequacy determination.¹¹² Mr. Schrems said, “Crucially, the EU constitutional framework requires independent oversight. The only way to change this would be a unanimous vote by all EU Member States to change the EU treaties.”¹¹³

It is not just the activist and civil society universe that is speaking out. The European Data Protection Board also sent a letter to the European Commission asking it to revisit adequacy in the wake of *Trump v. Slaughter*.¹¹⁴ The Board wrote that:

112. See *US Supreme Court Just Blew Up EU-US Data Transfers*, NOYB (June 29, 2026), <https://noyb.eu/en/us-supreme-court-just-blew-eu-us-data-transfers> [<https://perma.cc/J4HS-RJ5T>] (“EU treaty law (so the EU’s ‘constitutional’ framework), namely Article 16(2) [of the Treaty on the Functioning of the European Union] and Article 8(3) of the Charter of Fundamental Rights, requires that the oversight over data protection matters must be done by an ‘independent’ authority. Because third countries must have ‘essentially equivalent’ protections, it is necessary that any third country that wants to enjoy free flow of personal data from the EU also affords such protections. So far, the US has appointed the ‘independent’ FTC to be the US privacy regulator to meet the EU’s requirement for independent oversight. The EU, in turn, has relied on the FTC a whopping 259 (!) times in its [*sic*] EU-US data flow decision.”).

113. *Id.*

114. Letter from Eur. Data Prot. Bd. to Eur. Comm’n, *US Supreme Court Judgment Trump v. Slaughter* (July 31, 2026), https://www.edpb.europa.eu/system/files/2026-08/edpb_letter_20260731_us_supremecourt_judgment_trump_v_slaughter_en.pdf [<https://perma.cc/S6E9-CWVS>].

[T]he existence and effective functioning of one or more independent supervisory authorities in the third country, with responsibility for ensuring and enforcing compliance with the data protection rules, is one of the key elements to be taken into account when assessing the adequacy of the level of protection in a third country according to Article 45(2)(b) of Regulation (EU) 2016/679.¹¹⁵

Even if the European Commission itself agrees to uphold its adequacy finding, such a decision can—and certainly will—be challenged before the CJEU, which has twice invalidated adequacy before.

The implications extend beyond the European Union. Data transfer agreements, mutual recognition arrangements, and cooperative enforcement frameworks with data protection authorities around the world all depend on the good faith and institutional integrity of the American regulatory counterpart. When that counterpart is subject to direct political control, these frameworks are built on sand. The international architecture of data governance, painstakingly constructed over two decades of negotiation, is now threatened by a fundamental failure of American institutional design.

C. The Stakes for Democratic Dissent Globally

Location data and other commercial surveillance tools can be particularly pernicious when used to track and identify people engaged in constitutionally protected speech and assembly. The Mobilewalla complaint documented precisely this: The company had used its location data capabilities to compile profiles of persons who attended racial justice protests in summer 2020, including demographic analysis of protesters.¹¹⁶ The FTC took action against Mobilewalla, but did not dismantle the data infrastructure for this kind of political surveillance that continues to exist and be commercially available.

That danger of suppression of dissent is dramatically exacerbated when considered in global terms. American

115. *Id.*

116. See Mobilewalla Press Release, *supra* note 18.

platforms hold data on activists, journalists, dissidents, and opposition figures in countries around the world. That data could be extraordinarily valuable to authoritarian governments seeking to identify, track, and suppress political opposition. In many cases, the individuals most at risk are those who have engaged with American institutions, communicated with American journalists or officials, or participated in activities that attract the attention of their governments precisely because of their international connections.

The convergence of an unconstrained American executive with comprehensive American platform data holdings creates a new avenue for the exploitation of this data. Direct government-to-government demands for data, mutual legal assistance treaty requests, and informal intelligence-sharing arrangements all operate more freely when the data collection, concentration, and access are unchecked. And beyond direct government access, the mere existence of unregulated data broker markets means that non-US intelligence services, private surveillance companies, and politically motivated actors can purchase profiles of dissidents and activists from American commercial sources without triggering any meaningful legal review.

In combination, concentrated data holdings, politically controlled regulators, and a permeable border between commercial and governmental surveillance create the structural conditions for abuse on a global scale. The international community has a profound stake in the integrity of American regulatory institutions that it has perhaps not fully appreciated.

VI. TOWARD A FRAMEWORK: WHAT MUST BE DONE

A. Restore Independent Agency Protections

The most urgent structural need is the restoration of transparency and accountability in government institutions. In *Trump v. Slaughter*, the Supreme Court eliminated one mechanism that Congress has used for centuries to structurally ensure that transparency and accountability: removal protections. However, the Court did not say that the values of transparency and

accountability were unconstitutional.¹¹⁷ It is critical that voters install and demand a Congress that will exercise its own powers of oversight and its powers to structure agencies to be responsive and accountable to the American people.

This is not a partisan argument. The independence of regulatory agencies protects the public regardless of which party controls the White House. The largely partisan attack on agency independence ignores the fact that the foundational Supreme Court case protecting it involved a conservative Republican commissioner at the FTC, William Humphrey, who was fired for objecting to President Roosevelt's New Deal implementation.¹¹⁸ Democrats who value aggressive enforcement have the same structural interest in agency independence as Republicans who value corporate freedom. The degradation of independent agency protections does not benefit one side of the political spectrum; it benefits whoever holds executive power at any given moment, at the expense of everyone else.

The argument applies with particular force to the international dimension discussed in Section V. Foreign partners and trading partners cannot enter into meaningful data governance agreements with American regulatory agencies if those agencies are subject to instant political reconstitution. Restoring and codifying agency independence is a prerequisite for American participation in the international data governance architecture. That, in turn, should make it more appealing to the corporate institutions that are currently supporting the President.

117. For further discussion of the values historically guarded by removal protections, see Rebecca Kelly Slaughter, *The FTC After Trump v. Slaughter: A Joint Conference of the American Antitrust Institute and the Competition Law Center at the George Washington University Law School*, AM. ANTITRUST INST. (Aug. 3, 2026), <https://www.antitrustinstitute.org/wp-content/uploads/2026/08/Slaughter-Remarks-AAI-GWU-The-FTC-After-Trump-v.-Slaughter.pdf> [<https://perma.cc/U9J4-72LG>].

118. See *Humphrey's Executor v. United States*, 295 U.S. 602 (1935), *overruled by* *Trump v. Slaughter*, 146 S. Ct. 2883 (2026). President Roosevelt removed Commissioner William E. Humphrey, a conservative Republican appointed by President Coolidge and reappointed by President Hoover, over policy disagreements, notwithstanding the FTC Act's restriction of removal to "inefficiency, neglect of duty, or malfeasance in office." See *id.* at 618–19. The Court unanimously held that the FTC's quasi-legislative and quasi-judicial functions distinguished it from purely executive officers, and that Congress could constitutionally condition the President's removal authority. *Humphrey's*, 295 U.S. at 624–32.

*B. Comprehensive Federal Privacy Legislation with
Substantive and Structural Protections*

The United States remains one of the few developed democracies without a comprehensive federal privacy law. I have argued for such legislation throughout my time at the Commission, and the convergence of threats described in this Essay makes the argument more urgent than ever. A federal privacy framework must include several elements that existing sectoral law conspicuously lacks.

First, data minimization requirements: Companies should be prohibited from collecting data beyond what is necessary for the specific purpose for which it was collected, from using it for purposes other than those for which it was collected, and from retaining it when it is no longer necessary. These limits already apply to the government's direct collection of data for foreign intelligence purposes,¹¹⁹ and given the nexus that has evolved between government access and commercial collection, it is time to apply them to the private sector. Such a law would not merely protect individual privacy; it would reduce the concentration of data that makes corporate holdings so attractive as targets for government coercion. One cannot strong-arm access to data that does not exist.

Second, structural limits on government purchases of data: Congress should require judicial authorization for government purchases of commercially available personal data. The Fourth Amendment's warrant requirement should not be circumvented simply by routing government surveillance through commercial intermediaries.

Third, a private right of action: Privacy law enforcement cannot depend entirely on agency discretion when that discretion is subject to political capture. Individual rights of action create a resilient enforcement mechanism that cannot be turned off by replacing the FTC's commissioners.

119. FISA Section 702 requires the government to adopt minimization procedures "to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1).

C. Limits on Data Concentration

Competition policy has a significant impact on privacy policy. The concentration of data in the hands of a few dominant firms is a precondition for the architecture of coercion described in this Essay. The concentration that makes corporate data holdings so dangerous can be reduced through structural remedies, including merger enforcement, prohibitions on acquisitions of nascent competitors, or breakups, and substantive protections such as data portability mandates and privacy-protective interoperability requirements.

The FTC's years of work on Big Tech acquisitions, including the 2021 study of unreported acquisitions,¹²⁰ demonstrated that the problem is not merely one of inadequate enforcement of existing law, though that is part of it. The Hart-Scott-Rodino ("HSR") notification thresholds¹²¹ that allowed hundreds of data-accumulating acquisitions to proceed unreported need revision. The cases that have proceeded have not successfully broken up any large companies or meaningfully limited their market power. The substantive standard for anticompetitive data acquisitions needs development. And the structural remedy of data and model divestiture—requiring dominant firms to relinquish data holdings and any AI models built off those holdings as a condition of merger approval or as a remedy for anticompetitive conduct—needs to become a standard tool in the regulatory toolkit.

These competition interventions have direct privacy benefits. A market with more and smaller data holders is more resilient to government coercion; there would be no single dominant firm whose accommodation to government demands could yield comprehensive population surveillance. A more competitive market would be more responsive to consumer preferences; firms would face competitive pressure to offer genuinely privacy-protective alternatives. And such a market would be more amenable to meaningful consent. In a competitive market, consumers have realistic options, and their choices among those options have genuine meaning.

120. NON-HSR STUDY, *supra* note 5.

121. See 15 U.S.C. § 18a. The Hart-Scott-Rodino Antitrust Improvements Act of 1976 established the requirement that mergers over a certain dollar threshold be reported to the Federal Trade Commission before they can close, in order to give the government time to analyze the competitive implications of the transaction before it is consummated. See *id.*

D. International Models and Cooperative Pressure

The European Union's General Data Protection Regulation ("GDPR") and Digital Markets Act represent a structural choice fundamentally different from the American approach. The European model is rights-based, minimization-oriented, and enforced by authorities with sufficient independence and resources to pursue major platforms.¹²² The GDPR's adequacy mechanism has already proven to be a significant lever on American data governance. There is now a credible threat of adequacy withdrawal, meaning the European Commission or the CJEU could determine that American law no longer provides sufficient protection for EU data subjects. This may create pressure for reform that domestic politics alone may not generate.

But the international models also reveal the limits of external pressure as a substitute for domestic institutional integrity. The GDPR's effectiveness ultimately depends on the existence of an American regulatory counterpart capable of engaging seriously with data protection obligations. The Data Privacy Framework negotiated by the Biden administration was made possible because there were, at that moment, independent American regulators committed to its implementation, including at the PCLOB and FTC. Without such counterparts, the international framework becomes an arrangement between the EU and a White House that may or may not honor its commitments depending on the political calculations of the day.

International data governance therefore has a fundamental stake in the outcomes of *Trump v. Slaughter* and the broader struggle over the independence of American agencies. Non-US data protection authorities, international organizations, and multinational bodies should make clear that the degradation of American regulatory independence has direct consequences for international data governance arrangements. This can be achieved through formal legal interventions, adequacy reviews, diplomatic communications, and public statements. The international community cannot simply wait for American institutions to repair themselves. It should use the leverage it has.

122. See Aidun, *supra* note 104.

VII. CONCLUSION: THE STAKES

I began this Essay by noting that I write it as both a litigant and a regulator. That dual perspective has given me an unusually clear view of the stakes. The fight in *Trump v. Slaughter* was not, at its core, about one commissioner's job or even about the formal constitutional status of independent agencies. It was a fight about whether the institutions Congress created to check the most powerful actors in the economy, and to protect ordinary people from those actors, will continue to function, or whether they will be converted into instruments of the executive without any of the intended constraints.

The data concentration problem is similarly not, at its core, a fight about the business practices of specific companies or the adequacy of particular legal frameworks. It is a fight about whether the most intimate details of people's lives will be held in forms that make them accessible to anyone with sufficient power to compel or coerce access. When these two problems converge, as they are now converging in the United States, the result is a threat to personal privacy, and to the democratic participation, civil liberty, and human dignity that privacy enables, that is genuinely without historical precedent in its scope and sophistication.

None of these remedies is simple, fast, or comprehensive. All of them face determined opposition from interests that benefit from the current state of affairs. But the alternative of accepting the convergence of unchecked surveillance power and unbalanced market power as the new normal of American governance is untenable. It is a problem for democracy as much as it is a problem for privacy. And democracy problems, as history has repeatedly demonstrated, have a way of becoming everyone's problem, regardless of national borders.