Transparency Without Teeth: An Empirical Understanding of Data Broker Regulation

Elijah Greisz†

It is no secret that data has taken over the modern economy, and it is unsurprising that governments have begun acting in response. Perceiving mismatched bargaining power between firms and consumers—and certain externalities resulting from the massive quantities of data being collected by firms about those consumers—many state legislatures have passed generally applicable data privacy statutes. These laws give consumers certain rights to control the data they distribute in everyday commerce. Such regulations follow an "interaction model," whereby consumers can exercise their rights by interacting with data-possessing firms.

But there is a key player that complicates this scheme: the data broker. Data brokers buy and sell data about consumers with whom they never interact. They can have just as much—or more—data about a consumer as a traditional firm, but that consumer has no way to know that they do. How, then, is a consumer meant to exercise their rights with this "interaction gap" between them?

A handful of states have tried to soften the interaction gap by enacting data broker–specific legislation under the "transparency model." These laws, among other things, require brokers to publicly disclose themselves in state registries. The theory is that consumers would exercise their rights against brokers if they simply knew of the brokers' existence. California recently went further than the transparency model with the Delete Act, charting a new path for providing consumers data broker–specific privacy rights.

Assembling brokers' reported privacy request metrics, this Comment performs an empirical analysis of the transparency model's efficacy. It argues that privacy request usage rates demonstrate that the model does not do enough to facilitate consumers in following through on their expected privacy preferences. Regulators, if seeking to actually impact broker practices, must follow in the footsteps of the Delete Act and move beyond the transparency model.

† B.S. 2022, University of Washington; M.S. 2023, University of Washington; J.D. Candidate 2026, The University of Chicago Law School. I would like to thank Professor Lior Strahilevitz and the editors and staff of the *University of Chicago Law Review* for their thoughtful advice and insight.

INTRODUCTION

In the digital economy, money flows through data. Commentators have taken to describing data as the "new oil."[1] It is siphoned, sold, and shared. It is both abundantly generated by the technology industry and voraciously consumed by it. Quintillions of bytes of data—amounting to an almost inconceivable quantity of information, equivalent to over thirty-seven thousand times the size of the Library of Congress's book collection—are produced

[1] Kiran Bhageshpur, *Data Is the New Oil—and That's a Good Thing*, FORBES (Nov. 15, 2019), https://perma.cc/5ZY4-KYJL.

daily.[2] This encompasses nearly every facet of modern life: location data, purchases, searches, calls, messages, dating app swipes, and more.[3] In effect, every person leaves a digital footprint that very closely maps onto the fabric of their in-person life.

New industries, completely unknown to everyday consumers, have emerged to facilitate a market for this data, maximizing and capturing its value. Key to this emerging market is the data broker: a kind of company that purchases information from numerous others to assemble complete consumer profiles, and then sells access to those profiles for marketing or other purposes.[4] There might be little value to knowing a consumer's onetime Barnes & Noble purchase, but there is significant value to knowing the entire mosaic of their online interactions, the exact aggregation that brokers sell. This trade is not a function of the internet—it has, in essence, existed since the midcentury growth of the advertising industry—but data brokers have both been empowered by the rise of the digital economy and directly facilitated it. The sheer size of digital advertising, an industry valued at over $350 billion,[5] is a testament to brokers' significance. Some of the largest companies in the world generate empires of wealth through digital ads.[6] The result? An industry of brokers, some with data for billions of global consumers,[7] and an overall data broker market worth hundreds of billions of dollars.[8] In essence, data has fundamentally reshaped the modern economy, and data brokers have played an essential part.

---

[2] Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read. The Library of Congress has 25.77 million catalogued books in its collection, *General Information*, LIBR. OF CONG., https://perma.cc/2MTH-43NQ, and the average digital book file size is 2.6 megabytes, *Average Size of a Kindle Book*, ELITEAUTHORS (Nov. 18, 2020), https://perma.cc/FRJ8-CXND.

[3] Marr, *supra* note 2.

[4] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018), https://perma.cc/SR88-NTC6.

[5] Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the Internet*, N.Y. TIMES (June 23, 2023), https://www.nytimes.com/2021/09/16/technology/digital-privacy.html.

[6] *See, e.g.*, Nico Grant, *Alphabet's Revenue Jumps 15% to $80.5 Billion*, N.Y. TIMES (Apr. 25, 2024), https://www.nytimes.com/2024/04/25/technology/alphabet-earnings.html ("Alphabet continues to print tens of billions of dollars in profit from advertising each year.").

[7] *See, e.g.*, ACXIOM, ACXIOM DATA: LEVERAGE THE WORLD'S BEST DATA TO UNDERSTAND AND ENGAGE WITH PEOPLE EVERYWHERE 2 (2022) ("Acxiom's full scope of data and insights covers the globe with reach of 2.5 billion addressable people across APAC, EMEA[,] and the Americas overall.").

[8] *Data Broker Market Size & Share Analysis—Growth Trends & Forecasts (2025–2030)*, MORDOR INTEL. [hereinafter *Data Broker Market Size*], https://perma.cc/DLG7-SD26 (estimating the global data broker market size at $294.27 billion in 2025).

But such quantities of data—held by a handful of data brokers—have been put to controversial use. One former broker, which affiliated itself with consumer apps that targeted Muslim users, sold those users' location data to the U.S. military.[9] Another sold location data about abortion clinic visitors.[10] A third broker—now shuttered—recently suffered a security breach and lost an estimated 270 million Social Security numbers.[11] Thus, brokers' uses and abuses of the data they control range from normal activities in the ordinary course of trade to business failures reflecting serious incompetence. But in either extreme, the concern remains the same: What vulnerabilities emerge when a single firm has so much data about us?

In response to these concerns, states have passed legislation that empowers consumers by giving them some control over their data. The most famous example is the California Consumer Privacy Act of 2018[12] (CCPA), which allows people to learn about how their data is used and take actions to control the way it is processed—or even delete it outright.[13] Going even further, a handful of states have passed laws specifically tailored to data brokers, imposing additional requirements on them that go above and beyond the generally applicable privacy frameworks imposed on other firms.[14] The predominant design is what I call the *transparency model*: mandatory public disclosure of data brokers in a state registry, allowing consumers to exercise certain statutory privacy rights against such brokers. California has recently gone further and enacted the Delete Act,[15] providing consumers additional avenues to control their data.

---

9 Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://perma.cc/JL76-RD3J.

10 *Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics*, RON WYDEN: U.S. SENATOR FOR OR. (Feb. 13, 2024), https://perma.cc/V438-CP3E.

11 Zack Whittaker, *National Public Data, the Hacked Data Broker that Lost Millions of Social Security Numbers and More, Files for Bankruptcy*, TECHCRUNCH (Oct. 14, 2024), https://perma.cc/2U57-7UQB.

12 CAL. CIV. CODE §§ 1798.100–.199.100 (West 2025).

13 Jill Cowan & Natasha Singer, *How California's New Privacy Law Affects You*, N.Y. TIMES (Jan. 3, 2020), https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html.

14 *See infra* Part II.B.

15 CAL. CIV. CODE §§ 1798.99.80–.89.

Data broker regulation is an emerging area of law that is poised to grow in the coming years.[16] Legislators have increasingly turned their attention toward figuring out how to effectively regulate data brokers. Done correctly, such regulation could significantly empower consumers to better control the proliferation of their data across the digital sector. It could allow consumers to limit control of their data to only the firms they directly interact with. Done poorly, such regulation is mere symbolism without effect. At this crossroads, this Comment seeks to systematically analyze what makes for effective broker regulation.

This Comment presents a first-of-its-kind empirical evaluation of the effectiveness of existing data broker regulations. Taking advantage of a recent regulatory change effectuated by California's Delete Act, under which data brokers had to self-report privacy request metrics for the first time in 2024, this Comment assembles and analyzes a novel dataset comprising metrics collected from the 527 registered California data brokers.[17] This is the first set of data broker privacy metrics ever assembled. Analyzing this data, the Comment finds that relatively few consumers are exercising their privacy rights against data brokers. These low usage rates indicate that the transparency model—the predominant system of data broker regulation—falls short of serving as a real check on brokers' use of data. Based on this conclusion, this Comment urges regulatory innovation. If the law seeks to genuinely reshape consumers' relationship to their data, it must give consumers a mechanism to efficiently exercise their privacy rights. It does not yet do that. But the Delete Act will, and other states should follow suit.

Part I situates data brokers in the broader evolution of the data economy to show why they must be regulated differently from other types of firms. Part II details the landscape of data privacy regulation, including recent attempts by some states to specifically control data brokers. In doing so, it describes the transparency model and California's recent departure from it. Part III presents an empirical study of the transparency model's effectiveness, describing my methodology, dataset, and findings. Part IV turns those findings into concrete recommendations for

---

16 *See* David Stauss & Keir Lamont, *Retrospective: 2024 in State Sectoral Privacy Law and AI Law*, INT'L ASS'N OF PRIV. PROS. (Oct. 17, 2024), https://perma.cc/B62M-LKCH (describing how more states are considering data broker laws).

17 Elijah Greisz, Transparency Without Teeth Dataset [hereinafter Dataset], https://lawreview.uchicago.edu/media/850.

the regulatory landscape. Ultimately, the Comment provides empirical support for legislation, like the Delete Act, that moves beyond the transparency model, as that model appears to be an ineffective means of impacting broker practices.

I. THE DATA ECONOMY AND THE DATA BROKER

Before attempting to regulate the data broker—or deciding whether we should—we must take a step back and figure out what it actually means to be a data broker. Because brokers are unique in how they interact with consumers, ignorance of the differences between them is counterproductive to effective regulation—a pitfall of some of the regulatory models discussed in Part II. This goes beyond mere definition: it requires a careful examination of the contours of the modern data economy and the place that brokers have carved out. I begin this Part by providing a short history of the data economy and then discuss the emergence of the data broker within that economy.

A. A Short History of the Data Economy

Personal data found its first major, modern commercial use in advertising. In the early twentieth century, advertising agencies began creating market research departments to optimize ad campaigns.[18] Coinciding with a rapid increase in U.S. advertising spend, this was a differentiating competitive edge.[19] But data collection in those days was labor intensive: pollsters had to manually survey consumers to get answers, and consumers had to willingly and clearly provide such information for it to be of any use.[20] This labor intensity meant that the data's primary use was extrapolation, using the words of a few individuals to learn about society as a whole.[21]

Over time, advertising continued to drive the emerging data economy, but the data moved from being just about what consumers said to also what they did. This shift from

---

[18] Timandra Harkness, *The History of the Data Economy Part I: The Birth of Customer Insight*, 18 SIGNIFICANCE, no. 2, Apr. 2021, at 12, 12–13.

[19] *Id.* at 13 ("Advertising spend in the United States increased tenfold between 1900 and 1930.").

[20] *See id.* at 13–14.

[21] *Id.* (describing how early data use required using statistical sampling to learn about the population as a whole).

interrogation to *observation* meant that consumers were no longer necessarily aware of their data being used.[22]

The proliferation of computers across everyday life has drastically increased the scope of the data economy and dramatically augmented the capabilities of the observation approach. Data collection has expanded in the physical world—even fridges have become "smart."[23] In the digital world, nearly every website collects large quantities of data.[24] Given that the marginal cost of such digital collection is near zero, online companies have no reason not to collect it, and the result is them collecting unimaginable amounts of data.[25]

This pattern of practice has extended beyond online retail to other types of sites, and the value of data has enabled many companies to make extraordinary amounts of money from offering "free" services. For instance, Meta, known best for its social media platforms, by and large does not sell products to consumers but has over three billion active users worldwide—generating hundreds of billions of dollars in advertising revenue every year.[26] The value of this data is also due to its nature: social media users provide comparatively "new" information by discussing their day-to-day lives.[27] And while social media is the prototypical example, all internet sites have the potential to learn from user interactions

---

[22] *See* Timandra Harkness, *The History of the Data Economy Part II: Analytics Arrive*, 18 SIGNIFICANCE, no. 4, Aug. 2021, at 16, 19 ("[M]ethodologies have increasingly moved from being an 'active' process or collection to a passive, less intrusive, less conscious (and in some people's view, a more accurate) recording of behaviour and generation of information." (quotation marks omitted) (quoting ESOMAR, GLOBAL MARKET RESEARCH 2020: AN ESOMAR INDUSTRY REPORT (2020))).

[23] *See* Megan Case, *Google, Big Data, & Antitrust*, 46 DEL. J. CORP. L. 189, 196 (2022) ("[S]ources for big data continue to grow, including: smart home appliances and systems; health and wellness monitoring devices, commonly called 'wearables;' networked sensors; and geospatial technologies.").

[24] *See id.* ("The number of businesses and organizations with extensive data collection and processing capabilities are vast, including online and offline retailers, advertising networks, search engines, social networking sites, Internet service providers ('ISPs') and cable companies, financial institutions, insurance companies, data brokers, and government entities.").

[25] There is, of course, the cost of data storage. In the industry, this is often considered negligible compared to the data's future potential value. *See* Ben DeBow, *Where Is Your Data, and What Is It Costing You?*, FORBES (Dec. 11, 2023), https://perma.cc/G9W3-D3TL.

[26] *Meta Reports Fourth Quarter and Full Year 2024 Results*, META (Jan. 29, 2025), https://perma.cc/7M5D-GNVK.

[27] *See* Timandra Harkness, *The History of the Data Economy Part III: The New Kings and Queens of Data*, 18 SIGNIFICANCE, no. 5, Oct. 2021, at 16, 17 (discussing the optimism with which advertisers perceived social media as a form of acquiring new types of information from consumers).

and generate valuable data for advertisers. Large user bases serve both as valuable sources of data and captive audiences for advertisements. Consumer data, then, is valuable to websites both as an asset itself and as a means of optimizing their value to advertisers. This value is only increased when aggregated with data from other sources—creating a richer fabric of information.[28]

The arc of the data economy can thus be summarized in a few ways. First, the marginal cost of data acquisition has been minimized for three reasons: the move from interrogation to observation, the advent of increasingly digital interactions, and the decreasing costs of data storage.[29] Second, data has become more detailed, and hence more predictive, making it more valuable. This is mostly because of the vastly increased quantity of data resulting from lower acquisition costs. Such an increased quantity has a significant effect: more predictive power and more personalized advertising.[30] Third, data collection has moved from opt-in to opt-out. Rather than consumers voluntarily giving their data, consumer interactions are observed by default, oftentimes even without a consumer's awareness.

These three interconnected processes have taken the data economy from the fledgling advertising business of the early twentieth century to the three-trillion-dollar data economy central to commerce today.[31] But they have also fueled concerns about data privacy. These concerns first arose in the ordinary course of business, as the U.S. military and abortion clinic examples referenced above show.[32] In essence, this is data being used in normal commerce, but the potential harm is apparent, particularly when exploited against vulnerable groups. Even worse, this harm is magnified by data breaches, like the one that

---

[28] *See id*. at 19.

[29] *See* Thomas Coughlin, *Digital Storage and Memory Projections for 2025, Part 1*, FORBES (Dec. 6, 2024), https://perma.cc/W8LX-3WYT (showing that the price of hard disk drive storage in dollars per gigabyte has fallen by multiple magnitudes over the past twenty years).

[30] *See, e.g.*, Gunveen Ahluwalia, K. Senthamil Selvan, Dharmesh Dhabliya, Mahendra Kumar Singar, G. Ezhilarasan & Vaishali Singh, *Assessing the Benefits of Data Mining for Predictive Analytics*, 2023 IEEE INT'L CONF. ON EMERGING RSCH. COMPUTATIONAL SCI., at 1, 6 (finding that data mining can be used for predictive analytics, including for "personalized offerings . . . to target those customers most likely to buy their products or services").

[31] *See* Vasudha Thirani & Arvind Gupta, *The Value of Data*, WORLD ECON. F. (Sept. 22, 2017), https://www.weforum.org/stories/2017/09/the-value-of-data.

[32] *See supra* notes 9–10 and accompanying text.

compromised an estimated 270 million Social Security numbers.[33] In cases like these, we see how the sheer quantity of data collected can inevitably bleed into noncommercial life and be exploited by actors whose interests in no way align with those of the data subjects.

B. Data Brokers Finding Their Place

The data economy contains a spectrum of firms, ranging from what I call data-consuming to data-producing entities. Data-consuming firms have a use for data that they do not themselves collect. Data-producing firms are the opposite: they produce more data than they can directly use for their own products, like Facebook. This spectrum results in a robust data market, where the firm that finds some data to be the most valuable is often not the one directly collecting it.

The data market benefits from centralization. Data is most valuable when aggregated and demonstrably features economies of scale.[34] Combined with the need for data sharing, these dynamics push toward large data holders that make their data accessible to others in a bid to maximize its value. I offer two conceptual models for achieving this: internalizing data to collectors or externalizing it away from them.

Internalization means that dominant data collectors aggregate the data they collect and provide third parties some way to access its value without giving them the data itself. (In other words, the data is kept *internal* to the collector.) This is the model that Google and Meta have embraced.[35] Rather than sharing data, advertisers come to them, and these platforms then match advertisers to consumers. In effect, those with data needs are matched to those with data surpluses.

In contrast, externalization means that data-producing firms sell their data to third parties. The externalization model works best when a few firms buy significant amounts of data, aggregate it, and then sell access to data-consuming firms. That is the niche

---

[33] *See* Whittaker, *supra* note 11.

[34] *See* Dan Ciuriak, *The Economics of Data: Implications for the Data-Driven Economy*, CTR. FOR INT'L GOVERNANCE INNOVATION (Mar. 5, 2018), https://perma.cc/B45T-6NVJ ("[T]he initial investment cost to capture, assemble and process data is high, but the marginal cost of expanding data assets is very low. . . . [N]etwork externalities in the digital realm appear to be powerful, which tends to enable the emergence of natural monopolies or near monopolies.").

[35] *See Google Privacy Policy*, GOOGLE (Sept. 16, 2024), https://perma.cc/F8HF-DDZ5; *Privacy Policy*, META (Nov. 14, 2024), https://www.facebook.com/privacy/policy.

filled by data brokers. This, in effect, works similarly to the internalization model, but it additionally benefits data-producing firms with small data footprints that cannot productively aggregate internally. These smaller data collectors can sell to the brokers, and data-consuming firms can simply go to the largest brokers. Thus, the brokers serve as middlemen between those with data surpluses and those with data needs, reducing transaction costs.

This niche has proved highly valuable. Analysts have recently estimated the overall value of the data broker market to be near $300 billion.[36] Some brokers process data for billions of global consumers.[37] Large public companies—like T-Mobile, Experian, and TransUnion—have stepped into the brokerage market.[38] The result is a flourishing market of increasing economic value.

And as they have grown, data brokers have begun to enter public consciousness, often in moments of public concern.[39] Acxiom, an advertising company often labeled as the largest data broker in the world, gets attention in the press, often specifically about its mystique. One *New York Times* profile described it as the "quiet giant" that "peers deeper into American life than the F.B.I. or the I.R.S."[40] Such commentary illustrates a broader trend: consumers are becoming aware of data brokers' existence as an economic force, even if relatively few can name any individual brokers.

This increased awareness is motivated by greater concern about how brokers fit into society. Most famously, in 2018, the *New York Times* reported that the firm Cambridge Analytica improperly acquired the data of eighty-seven million Facebook users, creating voter profiles that could be used to target misinformation and influence elections.[41] Discovered shortly after Cambridge Analytica

---

36 *Data Broker Market Size*, *supra* note 8.

37 *See, e.g.*, ACXIOM, *supra* note 7.

38 *See* Dataset, *supra* note 17.

39 *See, e.g.*, Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. TIMES (Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html. This reporting caused enough controversy that General Motors stopped sharing data in this way. *See* Kashmir Hill, *General Motors Quits Sharing Driving Behavior with Data Brokers*, N.Y. TIMES (Mar. 22, 2024), https://www.nytimes.com/2024/03/22/technology/gm-onstar-driver-data.html.

40 Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

41 Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

claimed to have provided the "secret sauce" behind the 2016 U.S. presidential election,[42] this incident crystallized a burgeoning fear: the way in which consumer data can have very real and extraordinarily serious consequences outside of the digital sphere. As a result, there is mounting pressure for some constraints on how data is collected and used, including among brokers.

II. DATA PRIVACY REGULATION AND DATA BROKERS

As concerns over the data economy have grown, states have begun to erect a variety of regulatory structures. Due to their distinct attributes, data brokers are themselves a special piece of this regulatory puzzle. This Part begins by discussing the history of U.S. privacy regulation. At its core today is what I call the *interaction model*, where generally applicable data privacy statutes authorize consumers to exercise privacy rights by directly interacting with firms. Then, this Part details the more recent efforts to regulate data brokers specifically. The predominant approach is the transparency model, where states maintain public registries of brokers and require those brokers to disclose certain characteristics about themselves, with the hopes that this mandated transparency will change the brokers' conduct. By contrast, California's innovative Delete Act goes beyond the transparency model by providing consumers with data broker–specific privacy rights.

A. The Advent of Generally Applicable Data Privacy Statutes

Before data became the dominant economic force that it is today, U.S. privacy regulations were focused on protecting sensitive data. This Section chronicles the evolution toward generally applicable data privacy statutes—now dominant in many states—and explains how they encapsulate the interaction model.

1. Traditional privacy regulation based on the character of the data.

Early U.S. regulatory efforts at controlling commercial data privacy were focused on what were deemed as especially sensitive areas. Effectively, this focused on the *character* of the data. The

---

[42] Nicholas Confessore & Danny Hakim, *Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff*, N.Y. TIMES (Mar. 6, 2017), https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html.

first particularly sensitive use was creditworthiness. Insurance companies, creditors, and even employers could minimize the risk associated with a prospective associate by looking at their credit history, which included their income, past loan payments, employers, and more.[43] Much like data brokers today, credit bureaus filled a market need by assembling credit data about consumers across the United States. This data was highly sensitive because it had a significant effect on day-to-day life—it affected someone's ability to buy a house, get insurance, and even be employed. While this data was necessary to facilitate the modern, impersonal economy, its sensitivity meant that mistaken information could unjustifiably damage someone's life;[44] even worse, such information was prone to abuse.[45] The solution was the Fair Credit Reporting Act of 1970[46] (FCRA), which created a system of "due process" that empowered consumers to be aware of their credit reports and correct mistakes.[47]

While the FCRA was the first U.S. commercial data privacy law, subsequent regulations followed a similar model, protecting certain types of data categorized as especially sensitive. The Right to Financial Privacy Act of 1978[48] (RFPA) and the Financial Services Modernization Act of 1999[49] (RSMA) both focused on financial data, while the Health Insurance Portability and Accountability Act of 1996[50] (HIPAA) governed healthcare data. Generally, these laws have two aspects: they impose affirmative obligations on how private parties use personal information, and they give consumers rights to exercise some control over their personal information.[51] Still, these obligations and rights were

---

43 *See* G. Allan Van Fleet, Note, *Judicial Construction of the Fair Credit Reporting Act: Scope and Civil Liability*, 76 COLUM. L. REV 458, 458–59 (1976) (discussing how the modernizing economy became dependent on understanding consumer credits and credit reports).

44 A credit report with mistaken information could "destroy a person's ability to obtain credit, insurance[,] or even meaningful employment," and studies showed that "as many as one report in twenty may be materially inaccurate." *Id.* at 460–61.

45 Some credit bureaus attempted to "collect bills by threatening to ruin the debtor's credit rating." *Id.* at 460.

46 15 U.S.C. § 1681 et seq.

47 Van Fleet, *supra* note 43, at 466.

48 12 U.S.C. § 3401 et seq.

49 Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12, 15, 16, and 18 U.S.C.). This is colloquially known as the Gramm-Leach-Blilely Act.

50 Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

51 *See The Sedona Conference Data Privacy Primer*, 19 SEDONA CONF. J. 273, 362–78, 395–417 (2018) (summarizing the various federal health and financial privacy laws and their specific requirements).

restricted to specific types of data, leaving most data used in commercial life completely unregulated.

2. Recent generally applicable data privacy statutes and the interaction model.

Recently, some U.S. regulators—though not yet at the federal level—have moved beyond protecting only particularly sensitive data. The result is broader, generally applicable privacy statutes that apply to nearly all companies that collect personal information.

This started with California. After multiple unsuccessful attempts at federal generally applicable privacy legislation in the United States,[52] California voters proposed a ballot initiative to create such a law at the state level.[53] Concerned with some details of the ballot initiative, the state legislature rushed to supersede it[54] and passed the CCPA. Still dissatisfied with some of the details, the same consumer advocates got enacted another ballot initiative, the California Privacy Rights Act of 2020[55] (CPRA).[56] The resulting framework gives consumers rights over their data, including the right to delete personal information,[57] correct inaccurate personal information,[58] access their personal information,[59] know what personal information is sold and to whom,[60] opt out of their data being sold or shared,[61] and limit the use of sensitive personal information.[62] It also creates the California Privacy Protection Agency (CPPA) to manage enforcement.[63] Moreover, California's statute is generally applicable across all data types—

---

52 *See* Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS INST. (Jan. 14, 2021), https://perma.cc/N4KP-DNFE ("Congress failed to act in 2000, and still, over twenty years later, despite exhaustive debate and many dozens of bills and hearings, has failed to pass a comprehensive federal law protecting our data privacy and security.").

53 Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.

54 *Id.*

55 CAL. CIV. CODE §§ 1798.100–.199.100.

56 Sara Morrison, *California Just Strengthened Its Digital Privacy Protections Even More: Are Federal Privacy Laws Next?*, VOX (Nov. 4, 2020), https://perma.cc/G29K-XFLK.

57 CAL. CIV. CODE § 1798.105.

58 *Id.* § 1798.106.

59 *Id.* § 1798.110.

60 *Id.* § 1798.115.

61 *Id.* § 1798.120.

62 CAL. CIV. CODE § 1798.121.

63 *Id.* § 1798.199.10.

restricted only by thresholds for business size or activity.[64] Others followed suit: eighteen other states from across the political spectrum have comparable laws going into effect by the start of 2026.[65] This growing trend reflects the increasing political salience of data privacy.

Fundamentally, the CCPA and other state privacy statutes aim to give consumers some control as they interact with data-driven businesses in day-to-day life. If consumers frequent a website, they may want to opt out of having their collected data sold to others.[66] Or maybe consumers tire of using a platform and request that their data be deleted.[67] These controls are conceptualized as a byproduct of consumer-firm interaction: the interaction model. The core effect of these laws is to give consumers rights over their data—rights they can exercise only by directly interacting with data-collecting firms.

Of course, giving consumers privacy rights does not by itself influence the data economy. Any such effect depends on people actually exercising their rights, which in turn depends on them caring about privacy. The extent to which consumers care about privacy, then, is a foundational empirical question. Yet the evidence here is shaky at best. One well-known experiment demonstrated the "privacy paradox": consumers claim to care about privacy but then make choices inconsistent with those pro-privacy preferences.[68] A recent study looked at CCPA statistics and determined that privacy rights were exercised at relatively low rates, suggesting that consumers were similarly not taking advantage of privacy-conscious choices offered to them.[69] Why so? Scholars have offered different explanations for this paradox, including consumers' lack of knowledge, behavioral manipulation,

---

64 *Id.* § 1798.140(d)(1) (defining the thresholds that make the CCPA applicable to a business).

65 *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (last updated Jan. 6, 2025), https://perma.cc/8M73-QLPV.

66 *See* CAL. CIV. CODE § 1798.120.

67 *See id.* § 1798.105.

68 *See* Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 17–18 (Nat'l Bureau of Econ. Rsch., Working Paper No. 23488, 2017).

69 *See* Ella Corren, *Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Rights and Policy Implications*, 109 IOWA L. REV. 2017, 2042–45 (2024). This research is different than mine in that it focuses on large, consumer-facing firms—not brokers.

and friction in taking pro-privacy actions.[70] This Comment does not intend to provide any new answers here; rather, it attempts to frame how these potential causal factors—and the resulting paradox—may be amplified in the data broker context. This should be reflected, then, in the way that consumers behave toward data brokers, and it should be apparent in any data about such consumer behavior.

3. The interaction gap between consumers and data brokers.

The problem with the interaction model is that it does not easily translate to data brokers—a category of firms that consumers do not directly interact with. I call this problem the *interaction gap*. For traditional data-using firms, consumers know that the firm has their data. Nearly every Amazon user, for instance, knows that Amazon collects their data—after all, they enter it into the checkout form. The opposite is true for data brokers: without any direct interaction between users and brokers, users do not know when a broker has their data (or, sometimes, that the broker even exists). Without such knowledge, it becomes extraordinarily difficult for anyone to exercise their rights. How can one request that a firm delete their data if they do not know that the firm exists? This increases the friction already inherent in exercising privacy rights.

There have been some attempts to bridge the interaction gap and amplify the effectiveness of these laws on data brokers. For instance, under California law, when businesses receive requests to delete personal information, they must "notify[ ] all third parties to whom the business has sold or shared the personal information of the need to delete . . . unless this proves impossible or involves disproportionate effort."[71] In effect, businesses must "forward" delete requests to firms that they sold the data to. Yet there is no equivalent requirement to forward requests to correct, limit, or opt out.[72] This half measure raises questions about the

---

[70] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEORGE WASH. L. REV. 1, 11–22 (2021).

[71] CAL. CODE REGS. tit. 11, § 7022(b)(3) (2025).

[72] *See id.* § 7023 (lacking a requirement that businesses require third parties to correct the data that they shared with them); *id.* § 7027(g)(3) (requiring that businesses forward limit requests only to third parties that received sensitive personal information *after* the consumer submitted the request); *id.* § 7026(f)(2) (requiring that businesses forward opt-out requests only to third parties that received personal information *after* the consumer submitted the request).

ability of generally applicable data privacy statutes—as currently enacted—to affect the data broker sector.

B. Targeting Data Brokers with Regulation

Some states have gone further than generally applicable data privacy statutes and have passed laws specifically regulating data brokers. This Section starts by describing the prevailing transparency model before discussing California's recent innovation to that model.

1. The transparency model of most data broker regulation.

Responding to the interaction gap, four states—California, Oregon, Texas, and Vermont—each created a new type of data broker regulation grounded in the transparency model: public disclosure of data brokers.

Vermont acted first, through an unconventional legislative process that requested regulatory recommendations from the state's executive branch.[73] This resulted in a report that suggested, among other things, requiring data brokers to "employ reasonable security methods," "provide consumers with more information," and provide information about their practices to the Secretary of State.[74] In 2018, the state legislature effectively adopted these recommendations into law.[75] In short, Vermont's law aims, among other things, to solve the awareness problem by creating a public registry of data brokers and requiring them to disclose their practices.[76]

In 2019, California followed "in Vermont's footsteps"[77] and adopted comparable legislation. Like Vermont, it adopted a requirement that data brokers register with the Attorney General and disclose certain information about their data practices.[78] Unlike Vermont, however, California had a general privacy

---

[73] An Act Relating to Requiring Telemarketers to Provide Accurate Caller Identification Information, § 2(a)(2), 2017 Vt. Acts & Resolves 443, 446.

[74] OFF. OF THE ATT'Y GEN. & DEP'T OF FIN. REGUL., REPORT TO THE GENERAL ASSEMBLY OF THE DATA BROKER WORKING GROUP ISSUED PURSUANT TO ACT 66 OF 2017, at 25–26 (2017).

[75] *See* An Act Relating to Data Brokers and Consumer Protection, 2018 Vt. Acts & Resolves 584 (codified at VT. STAT. ANN. tit. 9, §§ 2430, 2433, 2446–2447, 2480b, 2480h).

[76] VT. STAT. ANN. tit. 9, § 2446 (West 2024).

[77] NICHOLE RAPIER, ASSEMB. COMM. ON PRIV. & CONSUMER PROT., AB 1202, at 7 (Cal. 2019).

[78] Act of Oct. 11, 2019, 2019 Cal. Stat. 6284 (codified as amended at CAL. CIV. CODE §§ 1798.99.80, .82, .84, and .88).

statute: the CCPA. This meant that consumers could, in theory, make privacy requests to brokers if they knew how to find them. The principal goal of this law was to fix the awareness problem and provide consumers a way to find brokers.[79]

In 2023, Texas and Oregon passed their own data broker registration laws. Both laws require data brokers to register with the state before doing business.[80] Like California, both states complement these data broker registries with general privacy statutes.[81]

All four of these statutes are principally focused on transparency. While they provide some additional protection—like requiring security measures or notice of data breaches—they are fundamentally defined by their requirement that data brokers move out from the shadows and register themselves with the state government. In three of these states—California, Oregon, and Texas—the registration requirement complements general privacy statutes that allow consumers to make privacy requests to a broker. In other words, it attempts to bridge the interaction gap.

But this is surely a fiction for most consumers. To exercise one's right to delete under the CCPA, for instance, usually requires filling out a Web form[82] and, sometimes, completing two-step verification.[83] It is one thing to believe that consumers will do this for websites they already frequently visit. It is another thing entirely to ask them to visit a data broker registry—mostly unknown to the public—and, one by one, make requests to data brokers. This is complicated by the fact that there is no way to know which data brokers have your data. If there are five hundred registered data brokers, must one submit a request to every broker, the vast majority of which will get rejected?

This is the potential puzzle of the transparency model. If the issue is that consumers are not aware of these data brokers—and thus are not able to exercise their rights—then making the

---

79 The legislature's bill analysis says as much. It states that "consumers need to know how to locate data brokers before they can take steps to exercise the particular rights granted under the CCPA." RAPIER, *supra* note 77, at 8.

80 An Act Relating to the Registration of and Certain Other Requirements Relating to Data Brokers; Providing a Civil Penalty and Authorizing a Fee, 2023 Tex. Gen. Laws 3089 (codified at TEX. BUS. & COM. CODE ANN. §§ 509.001–.010); An Act Relating to Registration of Business Entities that Qualify as Data Brokers; and Declaring an Emergency, 2023 Or. Laws 1035 (codified at OR. REV. STAT. § 646A.593).

81 *See* Texas Data Privacy and Security Act, TEX. BUS. & COM. CODE ANN. §§ 541.001–.205 (West 2023); Oregon Consumer Privacy Act, OR. REV. STAT. §§ 646A.570–.589 (2023).

82 *See* CAL. CODE REGS. tit. 11, § 7020(b).

83 *See id.* § 7020(d).

brokers accessible is a first step toward solving that. But how do people become aware of data broker registries? How do they know which brokers matter to them? Simply registering brokers does not seem to be enough. The problem is not just awareness: it is the distance between consumers and brokers. This throws the effectiveness of the transparency model into significant doubt; the model seems to assume a level of consumer awareness and sophistication that strains credibility.

2. Moving past the transparency model with the Delete Act.

Real solutions to the data broker problem must go further than registration requirements. The originally proposed version of the Texas statute, for instance, would have required that the Secretary of State maintain a "Do Not Collect" registry where consumers could submit a single request that required all data brokers to delete their data and cease collecting any more data about them.[84] Yet the bill got neutered through the legislative process, and this provision did not survive to enactment in Texas. U.S. senators tried to do something similar, proposing the federal DELETE Act.[85] The bill likewise would have required a centralized deletion system,[86] but it did not make it past mere introduction.[87]

Fortunately, California stepped forward—and even borrowed the name—creating its own Delete Act.[88] In fact, proponents in the state legislature acknowledged the exact problems described above,[89] stating that proper use of the registry "requires Californians to request each of the more than five-hundred registered brokers to delete their personal information."[90] The Delete Act's greatest innovation is that it requires the existing state data privacy agency, the CPPA, to develop a mechanism

---

84 *See* S. 88-2105, Reg. Sess., at 2–3 (Tex. 2023) (describing the creation of a "do not collect" registry).

85 S. 3627, 117th Cong. (2022).

86 *Id.*

87 *S.3627—DELETE Act*, CONGRESS.GOV (last updated Feb. 10, 2022), https://www.congress.gov/bill/117th-congress/senate-bill/3627/all-actions. The DELETE Act has been reintroduced twice in subsequent years, *see* S. 2121, 118th Cong. (2023); S. 1287, 119th Cong. (2025), but neither made it past introduction, *see S.2121—DELETE Act*, CONGRESS.GOV (last updated June 22, 2023), https://www.congress.gov/bill/118th-congress/senate-bill/2121/all-actions; *S.1287—DELETE Act*, CONGRESS.GOV (last updated Apr. 3, 2025), https://www.congress.gov/bill/119th-congress/senate-bill/1287/all-actions.

88 CAL. CIV. CODE §§ 1798.99.80–.89.

89 *See supra* Part II.B.1.

90 SEN. JUD. COMM., SB 362, at 11 (Cal. 2023).

through which a consumer can submit a single request to delete their personal information across *all* registered data brokers.[91]

The significance of this change cannot be overstated. In theory, it has the capacity to solve most of the transparency problem. Consumers no longer need to know which data brokers have their data—they just need to click one button. The time it takes to remove one's data from the broker ecosystem has been minimized. Furthermore, the Delete Act vastly expands the quantity of data that can be deleted. The CCPA requires that businesses delete data only if "collected from the consumer."[92] By contrast, the Delete Act requires deletion of "any personal information related to that consumer"—regardless of its source.[93] Large amounts of the data controlled by data brokers are collected from sources beyond consumers themselves, including public records and more. The Delete Act thus expands the domain of personal information over which consumers can exert their control.

Of course, the Delete Act has not escaped criticism. Some have argued that it will hurt small businesses and result in further concentration of the tech industry.[94] In a different vein, advertising companies objected that the Act's single delete mechanism is overly broad and robs consumers of choice.[95] But perhaps the most compelling criticism is that the Act jeopardizes the efficacy of some of the essential services that brokers sometimes provide, like anti–money laundering, sanction compliance, and cybersecurity services.[96] This is a debate in privacy more broadly,[97] but, if anything, such negative externalities are less severe in the data broker context. Because the vast majority of brokers' utility is in efficient advertising, increased privacy protection would likely affect pricing more than other externalities warranting greater caution. Furthermore, the existence of these

---

91 CAL. CIV. CODE § 1798.99.86.

92 *Id.* § 1798.105.

93 *Id.* § 1798.99.86(a)(2).

94 The argument is based on the premise that larger companies can more effectively absorb the cost of nontargeted marketing. *See* Dan Smith, *Opinion: SB 362—the 'Delete Act'—Will Hurt California's Small Businesses and Charities*, TIMES OF SAN DIEGO (Sept. 21, 2023), https://perma.cc/6ZBN-NCVK.

95 SEN. JUD. COMM., SB 362, at 17 ("This data broker deletion mechanism would rob consumers of the ability to elect not to do business with certain data brokers while choosing to engage with others.").

96 *See id.*

97 *See generally* Daniel J. Gilman & Liad Wagman, *The Law and Economics of Privacy*, 29 UCLA J.L. & TECH. 55 (2024) (discussing the economic trade-offs in privacy protections, particularly for the Federal Trade Commission).

externalities is a necessary trade-off of any meaningful reduction in data processing, and there are countervailing benefits to such a reduction, like economic justice.[98] Regardless, all these debates presuppose that privacy laws actually have an effect—good or bad. The existence of this effect is an empirical question that this Comment hopes to help answer.

The Delete Act goes into effect in stages. As of 2024, companies must register through the new registration process with the CPPA.[99] Toward the end of 2024, the CPPA began enforcement sweeps against unregistered brokers.[100] But the accessible delete mechanism—the core of the Act—does not go into effect until 2026.[101] In essence, then, the transparency model is still the only framework actively working today.

It is not hard to imagine that other states will begin to craft their own data broker laws in the image of the Delete Act—much like the process that followed California's enactment of the CCPA. In fact, 2024 saw some movement across a new set of states.[102] With regulation thus at a crossroads, it is crucial to carefully assess the various approaches. Some states may emulate the Delete Act, while others may simply stick with the transparency model—as Oregon, Texas, and Vermont have done. Before assessing the normative desirability of different approaches, we need to understand the real-world consequences of these approaches. In particular, we need to know whether the assumed deficiencies of the transparency model, discussed above, are actually realized.

III. EMPIRICAL EVALUATION OF THE TRANSPARENCY MODEL

The state of data broker regulation today raises important questions. The predominant regulatory approach falls under the transparency model—a model with questionable efficacy.[103] Does it go far enough to meaningfully empower consumers? That depends on the way the law affects brokers in practice. Thus, to

---

98 *See generally, e.g.*, Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice*, 52 ARIZ. STATE L.J. 368 (2020).

99 CAL CIV. CODE § 1798.99.82.

100 *See CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act*, CAL. PRIV. PROT. AGENCY (Oct. 30, 2024), https://cppa.ca.gov/announcements/2024/20241030.html; *CPPA Settles with First Set of Data Brokers*, CAL. PRIV. PROT. AGENCY (Nov. 14, 2024), https://cppa.ca.gov/announcements/2024/20241114.html.

101 CAL. CIV. CODE § 1798.99.86.

102 *See* Stauss & Lamont, *supra* note 16.

103 *See supra* Part II.B.1.

decide what the right regulatory approach to data brokers looks like, we need to first understand whether the current regime is having its intended effects.

The ultimate question, then, is how to measure the regulatory effects. Generally applicable privacy laws, which the transparency model complements, are grounded in a system of consumer rights. They affect businesses only to the extent that consumers *use* them to affect businesses. The same is true for brokers: brokers are affected only if consumers exercise privacy rights against them. The magnitude of the law's effect can therefore be measured by looking at how many consumers use their rights across the data broker sector. Furthermore, the relative effect across different brokers and different privacy rights—to delete, correct, access, and limit the spread of one's personal data—should illustrate how the law's effect varies in its application.

This Part first discusses a methodology for providing these answers and the first-of-its-kind dataset assembled pursuant to that method. It then uses the data to paint a picture of the way that consumers are currently exercising their privacy rights with brokers. This data appears to confirm that the transparency model is simply insufficient to dramatically impact the data broker ecosystem.

A. Developing a Methodology

To analyze the effects of current data privacy laws on data brokers, this Comment first develops and deploys a methodology to measure those effects. This necessarily has two component steps: identifying what firms count as data brokers under statutory definitions and examining those individual brokers to determine if consumers are actually exercising their rights against them.

Fortunately, the Delete Act provides a guide to both steps. California's data broker registration statute provides an authoritative set of all companies operating in the state of California that believe themselves to be subject to the Act. This is not necessarily coextensive with the set of data brokers that are required to register due to imperfect compliance,[104] but it provides an approximation of the set that we can work from.

---

[104] This can be overinclusive because some companies have chosen to register even though they claim they are not statutorily required to. *See, e.g.*, *Privacy Policy*, EMERGES.COM (Sept. 18, 2024), https://perma.cc/DK8L-DZ4P ("eMerges is not statutorilly

The second prong—the ability to analyze the impact of the law on individual brokers—is enabled by the Delete Act's requirement that data brokers annually report request metrics. Before the Delete Act, California regulations—promulgated under the CCPA—required that large data processors annually report specific metrics about CCPA rights usage.[105] This only applied to businesses that "buy[ ], receive[ ] for . . . commercial purposes, sell[ ], share[ ], or otherwise make[ ] available for commercial purposes the personal information of 10,000,000 or more" California consumers.[106] California has around forty million residents,[107] so this is a high threshold that requires a single business to interact with roughly a quarter of the state population's data in one year. Unsurprisingly, only a small group of businesses meet that threshold.[108] The Delete Act significantly expanded this reporting requirement and applied it to all registered data brokers[109]—defined to include any business that "knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[110]

The exact requirements of the metrics disclosure are defined in some detail. For each year that a company meets the statutory definition of data broker, they must register by January 31 of the subsequent year.[111] They then must report privacy metrics for the previous year by July 1.[112] These metrics must be disclosed "within the data broker's privacy policy posted on their internet website and accessible from a link included in the data broker's privacy policy."[113] The following provision states the exact numbers required to be included:

[sic] required to register as a California Data Broker but does so voluntarilly [sic]."). It can be underinclusive because some companies likely meet the statutory definition but have not registered. This possibility is made more likely based on the number of brokers that registered late, *see infra* text accompanying notes 128–32, and the fact that some brokers are inconsistently registered across states, *see infra* Part III.C.2.

105 CAL. CODE REGS. tit. 11, § 7102(a).

106 *Id.*

107 *See QuickFacts: California*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/CA/PST045224.

108 One recent study found 137 firms that reported in 2020 and 121 in 2021. Corren, *supra* note 69, at 2034.

109 CAL. CIV. CODE § 1798.99.85.

110 *Id.* § 1798.99.80(c). This does not include firms that are entirely covered by certain other privacy laws, like the FCRA, and firms that only process data in ways that are exempt from the CCPA. *Id.*

111 *Id.* § 1798.99.82(a).

112 *Id.* § 1798.99.85.

113 CAL. CIV. CODE § 1798.99.85(a)(3).

> (1) Compile the number of requests pursuant to [the Delete Act's Accessible Delete mechanism] and [the CCPA sections relating to the rights to delete, know, opt out, and limit] that the data broker received, complied with in whole or in part, and denied during the previous calendar year.
> (2) Compile the median and the mean number of days within which the data broker substantively responded to requests pursuant to [the Delete Act's Accessible Delete mechanism] and [the CCPA sections relating to the rights to delete, know, opt out, and limit] that the data broker received during the previous calendar year.[114]

Reading the statute in isolation, it is unclear whether this disclosure requires a single number for all request types or a different number for each request type. The CCPA regulations require the latter,[115] so one might assume that the same is true here. In practice, different businesses take different approaches,[116] and subsequent regulations have not provided any additional clarity.[117] Regardless, these numbers provide some quantitative measure of how current California privacy laws are affecting data brokers.[118]

In short, the reporting requirements under California law enable both prongs of an empirical inquiry: they provide some way to identify data brokers and a way to determine the extent to which consumers are exercising their privacy rights against such brokers. Given that the Delete Act went into effect on January 1, 2024, the first broker registrations were due by January 31, 2024.[119] Each of those registered brokers was required to post their 2023 metrics to their privacy policies by July 1, 2024.[120] Notably, this only includes requests made under the CCPA—the Delete Act's accessible delete mechanism does not go into effect

---

114 *Id.* § 1798.99.85(a)(1)–(2).

115 CAL. CODE REGS. tit. 11, § 7102(a).

116 *See infra* Part III.C.1.

117 CAL. CODE REGS. tit. 11, §§ 7600–7605.

118 Because there is no audit mechanism yet in place, some firms might report false numbers. But there seems to be little incentive to do so because the reported metrics are seemingly not used by the government for any other purpose. Without the metrics being used for some tangible, economically impactful effect, brokers are unlikely to intentionally misreport.

119 *See* CAL. CIV. CODE § 1798.99.82(a).

120 *See id.* § 1798.99.85(a).

until 2026.[121] Therefore, these numbers solely reflect requests made under the transparency model.

B. The 2023 Dataset and Its Limitations

Using the parameters discussed in the preceding Section, this Comment compiles, to my knowledge, the first set of Delete Act metrics ever assembled. It is both a source of data for contemporaneous analysis, as demonstrated in the next Section, and a baseline for metrics in future years.

Following the method described above, I first extracted the list of California data brokers from the CPPA and subsequently visited each website to search their privacy policies for their self-reported 2023 metrics.[122] I then assembled these metrics into a single dataset.[123] This dataset includes the 527 data brokers registered with the CPPA at the time of data collection on November 15, 2024.[124]

---

[121] *See supra* note 101 and accompanying text.

[122] I retrieved the list of California's registered brokers from the CPPA's website on November 15, 2024. *See Data Broker Registry*, CAL. PRIV. PROT. AGENCY, https://perma.cc/4R3D-A9J7. Each broker in this list reports a link to a place on its website that describes how consumers can exercise their California privacy rights. This part of the website also generally contains its Delete Act metrics report.

For each broker, I visited the link described above and searched for its reported Delete Act metrics. If I could not find them on that page, I then searched any page on the broker's website labeled "Privacy Policy," "California Privacy Rights," "Additional State Disclosures," or something similar. If I could find request metrics reported on any of these pages, I collected the data for that broker.

While assembling the data, I preserved its reported categorization as much as possible. Some brokers reported a single number (e.g., "Total Requests Received"), while others reported different metrics for each type (e.g., "Requests to Know Received"). Each variety was translated directly into the data. There are two primary exceptions to this. First, if a broker reported a conjugation of some subset of privacy rights, I added that number to *each* constituent privacy right. For example, if a broker reported ten "Requests to Know and Delete," I counted that as ten requests to know and ten requests to delete. This is not analytically different than a consumer submitting a privacy Web form and selecting multiple types of requests at once—both represent one consumer exercising multiple rights simultaneously, so they were counted the same way. Second, if a broker reported a disjunction of a single privacy right, I added those constituent pieces to calculate the total number for that specific right. For instance, if a broker reported 10 requests to opt out submitted via email and 1,000 submitted via a form, I simply recorded that 1,010 requests to opt out were submitted.

While I generally sought 2023 metrics, some data brokers reported metrics for other time periods. For instance, some included inexplicable date ranges, like January 1, 2023, to August 20, 2024. For all such cases, I erred on the side of overinclusion for subsequent analysis, figuring that some data about a broker was better than none, even if it was not quite "2023" data.

[123] Dataset, *supra* note 17.

[124] *Id.*

Before looking at the substance of the reported metrics, I must take a step back and comment on the dataset as a whole. These brokers range from well-known companies like T-Mobile to lesser-known companies like Acxiom.[125] They include political mobilization companies, credit bureaus, and artificial intelligence companies.[126] In other words, the included data brokers themselves run the gamut of economic life.

Several limitations of the dataset bear mention. First, this data represents only a single year. Consumer and data broker metrics for 2023 may not be representative, so this Comment's findings should be understood as showing a snapshot in time. This is particularly true because data broker laws are becoming more salient, and the Delete Act in particular went into effect recently.[127] As consumers and brokers come to better understand this area of the law, the data may look substantially different in subsequent years. Second, this data comes from the state of California and so may not be representative of other states. Third, this data reflects the preferences of those *already* making privacy requests. We cannot assume exact symmetry with those who have yet to make requests. Privacy-conscious consumers are distinctly different than privacy-clueless consumers, and the idiosyncratic preferences of one cannot be transposed onto the other. This effect is made more pronounced by the fact that individual users could potentially be submitting multiple requests. Regardless of these limitations, however, this dataset is still useful in representing what is happening right now: who presently makes requests and which brokers are actively receiving them.

C. Empirical Results

This Section draws out findings from the brokers' self-reported data. These broadly fit into two categories. The first category reveals issues of compliance, both within California and across each of the other three state registries. This principally speaks to issues with the law's enforcement, but such noncompliance also imposes methodological limitations for any substantive analysis about the efficacy of the transparency model based on this data.

---

125 *Id.*

126 Examples include BlueAction, TransUnion, and Sterling.ai. *Id.*

127 *See supra* notes 99–101 and accompanying text.

The second category of findings includes three observations from the brokers' self-reported data, each speaking to the effect of the transparency model on data brokers in California. First, different brokers receive different quantities of consumer requests; this seems to be due to factors beyond just the brokers' size, such as the diversity of their business and technological models. Second, while there is significant variation, consumers tend to prefer to exercise their rights to delete and opt out for brokers, with the right to opt out counterintuitively being more popular than the right to delete for most brokers. Third, many brokers receive fewer requests than comparable consumer-facing firms.

1. Compliance has been difficult and uneven within California.

Immediately evident from the data is the fact that California data brokers have struggled to comply with the Delete Act in its first year. A significant portion of companies seemingly registered late. Of the 527 brokers, 409 registered in January 2024.[128] This means that 118 registered after the statutory deadline of January 31.[129] One might hypothesize that these late registrants are likely unsophisticated actors, but that is not exclusively the case. For example, Deloitte, one of the largest accounting and consulting firms in the world,[130] registered their financial advising subsidiary on February 26.[131] These cases are particularly puzzling. The most likely explanation is the Delete Act's recency, so perhaps some grace should be extended to these mistakes. This seems to be the approach that the CPPA took, as it did not start enforcement sweeps until October 30, 2024—nearly nine months after the registration deadline.[132]

Moreover, many brokers had yet to publish metrics well after the July 1 deadline. Only 293, a bare majority, had metrics posted on their website as of the middle of November. Even just among

---

[128] Dataset, *supra* note 17.

[129] Maybe some are trying to register very early for commercial activity performed in 2024. This would be a mistaken interpretation of the statute: they must register the "following year," which suggests that they cannot register while the year is still going. CAL. CIV. CODE § 1798.99.82(a). Regulations passed at the end of 2024 confirmed this—the registration period is January 1 to 31. CAL. CODE REGS. tit. 11, § 7601(d).

[130] Jason Bramwell, *Deloitte Global Hauled in $67.2 Billion in Revenue This Year*, CPA PRACTICE ADVISOR (Sept. 13, 2024), https://perma.cc/2GDY-8SAB.

[131] Dataset, *supra* note 17.

[132] *CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act*, *supra* note 100.

the firms that registered on time—and thus seem to be more on top of their legal obligations—only 63.5% (260 out of 409) published their metrics by mid-November 2024.[133] Of all registered brokers, 44% were engaged in facial violations of the statute by not reporting metrics;[134] they included even seemingly sophisticated actors like Moody's, a large financial services corporation.[135] This may be explained in part by the temporal gap between registration, in January, and metrics posting, in July. Brokers may realize they need to be on top of their registration at the beginning of the year, but conscious awareness may slip by as the year progresses. It is also possible that the CPPA's relaxed enforcement—and a feeling that the metrics reporting is an ancillary part of the law—meant that brokers simply decided it was not worth doing. They may be especially incentivized to "forget" to report if they believe that the CPPA is using such reporting to target its enforcement.

Other firms attempted to report metrics but failed to do so properly. Many reported statistics for the wrong time period. Some had metrics that were too old,[136] while others had metrics that were too new.[137] Some provided incomplete metrics.[138] Some had numbers that are just not possible—for instance, reporting more instances of compliance with a given request than the number of such requests received.[139] The number of blatant errors indicates that some brokers are either being careless or intentionally misreporting statistics,[140] suggesting that they are not taking the metrics provision as an essential attribute of the law and that the CPPA is not enforcing it.

Even among brokers who do report plausible numbers, seeming to comply with the law's requirements, there are massive

---

[133] Dataset, *supra* note 17.

[134] CAL. CIV. CODE § 1798.99.85.

[135] Dataset, *supra* note 17.

[136] *See, e.g.*, *SheerID Global Privacy Policy*, SHEERID (Nov. 5, 2024), https://perma.cc/FF9F-RAKM (reporting data subject requests for 2022).

[137] *See, e.g.*, *CCPA Privacy Request Metrics*, S&P GLOB., https://www.spglobal.com/en/legal/ccpa-privacy-request-metrics (reporting metrics for the period between January 1, 2023, and August 20, 2024).

[138] *See, e.g.*, *Our Privacy Policy*, RECRUITBOT (June 28, 2024), https://perma.cc/K2KH-M3YF (identifying the average response times that the company must report under the Delete Act but not including request numbers).

[139] *See, e.g.*, DUN & BRADSTREET, CALIFORNIA RESIDENT SUPPLEMENTAL DISCLOSURES 15 (2024) (stating that thirteen requests to know were received but fourteen were complied with).

[140] As stated before, I believe intentional misreporting is unlikely. *See supra* note 118.

differences in the manner of reporting—mostly due to the statutory ambiguity discussed above.[141] Brokers either report a single number for all requests or report different numbers for each request type.[142] They either report the median or mean number of days to respond, and some do both.[143] These differences reveal the issues with ambiguous statutory requirements. They also make data analysis more methodologically difficult.[144]

The variation most worthy of comment is in jurisdiction. The statute itself is not expressly clear but suggests that brokers should be reporting metrics only for Californian consumers.[145] The vast majority of brokers report metrics without stating the jurisdiction, so, for present purposes, I assume for them a default of just California. But 13%[146] expressly state that they are reporting for broader jurisdictions.[147] This limits much of my subsequent analysis. First, I cannot directly compare the number of requests received from a California-reporting firm to a non-California-reporting firm. Thus, I limit my analysis to California-reporting firms. Second, some brokers might not expressly state a jurisdiction yet still report for a broader jurisdiction than California—there is simply no way to know. If my assumption that these metrics pertain only to California had a systematic effect, it would be overestimating the relative usage of privacy rights, which would only compound my core conclusion that such rights are hardly used.

In short, many brokers have struggled with proper compliance. Some have outright statutory compliance failures: they registered late, failed to post metrics, or posted noncompliant metrics. Even among those that did comply, there is massive variance in the way that companies disclose their metrics. These issues complicate my subsequent findings. For one, variance

---

141 *See supra* text accompanying notes 115–17.

142 *Compare Privacy Policy*, SALUTARY DATA (May 8, 2024), https://perma.cc/LG7H-GUQ4 (reporting just one number for the sum of all requests), *with U.S. Data Product Privacy Notices*, ACXIOM (Dec. 31, 2024), https://perma.cc/5U4C-LRS5 (reporting different numbers for each request type).

143 *See, e.g.*, *U.S. Data Product Privacy Notices*, *supra* note 142.

144 These differences make it hard to aggregate statistics across the data, which removes some of the value that the quantitative nature of the metrics provides.

145 The statute asks for metrics developed pursuant to various CCPA provisions, and those CCPA provisions and rights are applicable only to California consumers. *See* CAL. CIV. CODE § 1798.140(i) (limiting the definition of "Consumer," the subject of the Delete Act's metric reporting requirements, to "California resident[s]").

146 This is 34 of the 256 reporting brokers. Dataset, *supra* note 17.

147 *See id.*

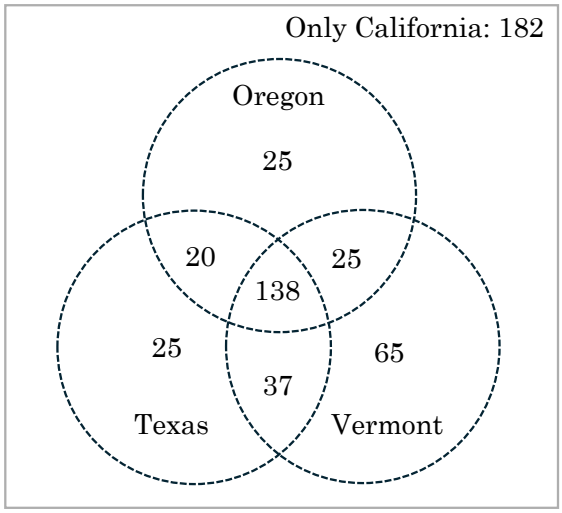
across reporting methods strains the inferential ability of comparative analysis. It is hard to compare two brokers if they report metrics in different ways. Second, noncompliant firms failing to report metrics reduces the sample of metrics that I can analyze. A smaller sample makes the data less capable of representing the broker sector more broadly. Moreover, beyond the implications for my own analysis, these compliance issues demand both greater enforcement of the law and clearer guidance for regulated parties.

2. Brokers are not consistently registered across all state registries.

Three other states—Oregon, Texas, and Vermont—require registration, but their registries are each substantially different in content. In other words, different data brokers register in different states, and most data brokers do not register in all states. Figure 1 presents how many California brokers are registered in each combination of other states. For example, there were twenty brokers registered in California, Oregon, and Texas, but not in Vermont.[148]

[148] *Id.*

FIGURE 1: NUMBER OF CALIFORNIA BROKERS REGISTERED IN OTHER STATES[149]



This is a puzzling result given the fact that data brokers typically operate across the internet, which spans all states. Other than the 138 brokers that are in all four registries, the remaining 389 California brokers instead register across some patchwork of states.[150] This could partially be explained by slightly different statutory definitions—particularly Texas's, which has the highest applicability threshold[151]—but it does not explain all these

---

[149] I downloaded the data from the Oregon, Texas, and Vermont state data broker registries and integrated them into the dataset. *See id.* For each of California's registered brokers, I searched for the closest match registered in each of the other states. In this search, I looked for both the business name and the "doing business as" name. This was completed across two phases: I first created a program to automate the matching, and then I cross-checked each broker to catch misses and ensure the accuracy of hits. In my data, then, each broker has a column containing its corresponding name in each other state registry.

This mapping was not always one-to-one. TransUnion, for instance, has five "TransUnion *X*" (e.g., "TransUnion Digital LLC") brokers registered in California, but only registers as "TransUnion Risk and Alternative Data Solutions, Inc." in Texas. In this case, I counted all five California brokers as being "included" in the Texas registry, and each of the five mapped to this one Texas broker in the dataset. *Id.*

After doing this for all California brokers, I assembled the number of California brokers registered in each combination of the four states. *See* Dataset, *supra* note 17. Those numbers were then made into this Venn diagram.

[150] *Id.*

[151] Texas's statute applies only to brokers that derive more than 50% of their revenue from data they did not directly collect or that derive revenue from processing or transferring the data of more than fifty thousand Texans that was not directly collected by the broker. TEX. BUS. & COM. CODE ANN. § 509.003.

differences. For example, sixty-two brokers registered in Texas but not Oregon,[152] despite Oregon having a strictly weaker definition of broker.[153] And some of these are large companies for which we would expect sophisticated legal compliance.[154]

This points to a concern about the state-by-state approach: it multiplies compliance costs, making it relatively difficult for companies to become compliant everywhere they operate—which is to say, everywhere with a registration requirement. The internet is what distinguishes these registration laws from those applied to other sorts of businesses, where a firm must generally choose to do business in a state in order to be subject to its regulations, selecting into a given compliance regime. Given the nature of data brokers' business, every new state registration requirement will apply to them more or less automatically, depending on whether the state imposes thresholds on the regulation's applicability. In a world where all fifty states require registration, for instance, companies would have to spend significant amounts of time and money registering in each state. Even with just four state registries, middlemen companies have already formed to manage the compliance process.[155] Again, we can highlight Moody's—a significant financial services corporation that has registered only in two out of the four states.[156]

The fact that broker registration varies by state has two immediate implications, one methodological and the other legal. First, it emphasizes that the dataset might itself be underinclusive. Just as there are many firms not registered in Oregon despite statutory requirements, some firms likely are not registered in California. Noncompliant firms are not captured by this data. Second, these differences across states offer a clear place to start enforcement sweeps. If these laws are to have any effect, governments must be proactive in enforcing against unregistered,

---

152 Dataset, *supra* note 17.

153 Oregon requires only that a business sell or license brokered information—not that it meet some threshold of revenue or users. OR. REV. STAT. § 646A.593.

154 For example, Samba TV is registered in California, Texas, and Vermont, but not Oregon. Dataset, *supra* note 17. Its business arrangements suggest legal sophistication. *See Home*, SAMBA TV, https://perma.cc/JK7B-7VE4 (describing its partnerships with many TV brands, including Sony, and its "48 million" TVs).

155 *See, e.g.*, Zane Witherspoon, *Understanding Data Broker Regulations in the U.S.*, SUPERSET (Aug. 21, 2024), https://perma.cc/TS5F-CY58 (promoting the services of Superset as a registration agent to assist with data broker law compliance).

156 Moody's registered in California and Oregon but not Texas or Vermont. Dataset, *supra* note 17.

noncompliant brokers. Looking at other state registries provides a clear pool of brokers who have potentially evaded registration.[157]

3. Data brokers receive vastly different quantities of requests, and the reason seems to go beyond size.

As expected, there is great variance across the number of requests that different brokers receive from users each year. This variance is demonstrated in Table 1. Each row represents a range, and the table presents the number of data brokers that received a total number of requests within that range. For instance, the second row of data indicates that seventy data brokers reported receiving somewhere between one and ninety-nine total requests in 2023.[158]

---

[157] These interstate differences also suggest that states could coordinate—perhaps through a shared registration system—to make both enforcement and compliance more efficient. Alternatively, a single federal law could accomplish the same ends. The details of such coordination or legislation are outside the scope of this Comment.

[158] To restrict my comparison to firms reporting metrics for the same jurisdiction, I excluded brokers who stated that their metrics represented jurisdictions broader than just California. This left 222 metrics-reporting brokers. Dataset, *supra* note 17.

For each of these brokers that directly reported the total number of requests it received, that number was used to determine its bucket. If a broker did not directly report the number of total requests, I added up the reported number of requests to know, delete, correct, limit, and opt out to create a synthetic total, and I then put that broker in the corresponding bucket. One limitation of this second approach is that some firms potentially combined request types. For instance, VenPath reported 182,167 delete requests and 182,167 opt-out requests. *Id.* It is plausible that VenPath combined delete and opt-out requests so that these represent only 182,167 unique requests, and they would be double-counted under my approach.

TABLE 1: NUMBER OF BROKERS
RECEIVING DIFFERENT QUANTITIES OF REQUESTS

Total Number of Received Requests	**Number of Data Brokers**[159]
0	21
1 to 99	70
100 to 999	42
1,000 to 9,999	34
10,000 to 99,999	35
100,000 to 999,999	13
1,000,000 to 9,999,999	6
10,000,000 to 99,999,999	1
Total	**222**

These numbers provide a sketch of the data broker economy. If request volume was linearly correlated with the quantity of personal information processed, this would also provide an approximate map of the largest data brokers and the oligopolist tendencies that one might expect.[160] In fact, the most-requested broker—representing less than 1% of the 222 brokers included in the analysis—reported receiving roughly 43% of the total reported requests.[161] The top six report receiving over 80% of all reported requests.[162] This conclusion could help target regulatory approaches: those brokers with the greatest difference between their market power and reported metrics are likely the ones imposing the greatest friction on consumers.

---

[159] Some companies have multiple data broker subsidiaries that are each registered but report only a single set of metrics for the entire company. One example is Experian. *Id.* In all subsequent analysis, if a subsidiary or sister company does not report its own statistics, it is not included as a separate broker. This can get complicated. TransUnion, for example, has eight brokers in the dataset. Seven report a single set of metrics (included in TransUnion's privacy policy), while its subsidiary, Neustar, reports a different set of metrics (on its own privacy policy). For my calculations, the seven count as one broker, and Neustar counts as a second broker. *Id.* Otherwise, it is impossible to know how the requests are distributed across the seven, and it is incorrect to assume that each of the seven shares an equal portion of the requests.

[160] Because data benefits so heavily from economies of scale, one might expect that the largest data brokers provide significantly more value to their customers. This feedback loop results in concentration of market power.

[161] A total of over 33 million privacy requests were reported across all brokers, and over 14.5 million of these came from the top reporting broker. Dataset, *supra* note 17.

[162] Over twenty-six million requests were received by the six largest brokers, out of a total of thirty-three million requests. *Id.*

The issue is that these numbers do not seem to strongly correlate with the relative sizes of brokers. While all large request receivers necessarily have large amounts of data, not all large brokers are large request receivers. The clearest example is Acxiom, which is one of the largest data brokers in the world.[163] It only received roughly seventy-seven thousand requests in 2023, making it the twenty-third largest broker by request count (of those who reported only California requests). The number one firm by requests received—Experian's subsidiary Tapad[164]—reports nearly two hundred times as many requests as Acxiom, primarily driven by over fourteen million opt-out requests.[165] This cannot simply be a function of the quantity of data, given Acxiom's size.

What can explain the drastic, fourteen-million-request difference in opt-out requests between the two firms? Tapad's privacy policy states that Tapad runs in mobile applications and can accept opt-out requests through a phone's device settings.[166] Therefore, it might be that many consumers use apps supported by Tapad's advertising platform and independently opt out in their phone settings. While it is impossible to know whether this is the actual cause of the difference, it does raise the possibility that Tapad's metrics are not evidence of the transparency model working; rather, it might just be that certain external mechanisms soften the interaction gap for a subset of brokers.

One can also look at the broker Cuebiq, which reported over forty-three million global privacy requests.[167] Because Acxiom reported only numbers for California, one cannot directly compare the numbers themselves. But one can compare the proportions—which are striking. Acxiom, in California alone, had roughly ten times as many requests to know and five times as many requests to delete than Cuebiq had *worldwide*.[168] But Acxiom had nearly six hundred times *fewer* requests to opt out. The opt-out numbers

---

[163] *These Are the Largest Data Brokers in America*, PRIVACYBEE, https://perma.cc/WJM5-U7YN.

[164] Experian collectively reports a total of 14.5 million requests received in 2023, *see* Dataset, *supra* note 17, but over 14 million of them came from their subsidiary Tapad. *See U.S. Consumer Data Privacy Policy*, EXPERIAN (Nov. 1, 2024), https://perma.cc/N3WP-LP9G.

[165] Dataset, *supra* note 17.

[166] *See Privacy Notice—Global*, TAPAD (Jan. 22, 2025), https://perma.cc/P89V-W2AD ("To adjust your advertising preferences in Android, visit Settings > Google > Ads > Opt out of interest-based ads or Settings > Google Services & Preferences > Ads > Opt out of Ads Personalization.").

[167] Dataset, *supra* note 17.

[168] *Id.*

suggest consumers are extraordinarily interested in exercising their rights against Cuebiq, but the delete numbers reflect extraordinary disinterest. How can one reconcile the two?

The most plausible, if tentative, explanation is that it simply comes down to the different way that Cuebiq interacts with its data providers and accepts opt-out requests. Cuebiq is an Application Programming Interface (API) designed to be directly used by app developers.[169] It requires opt-in advertising sharing via a user's device (imagine a pop-up asking to share information) and suggests that one method for consumers to opt out is to limit the app's advertising tracking.[170] In other words, a user does not need to directly interact with—or know about—Cuebiq in order to opt out. By contrast, Acxiom's only described opt-out methods are online form submission, mail, or phone.[171] Simply put, these brokers are different types of technological firms and thus are impacted differently. Cuebiq is seemingly swept into the interaction model, where direct consumer interaction with platforms reaches the broker's activities, and Acxiom is not, remaining subject only to the transparency model. In short, it seems that Cuebiq's business model may impose less of an interaction gap with consumers than Acxiom's, resulting in less friction for consumers to exercise their privacy rights.

While these pairwise comparisons are not necessarily representative of the broader dataset, they do emphasize a basic but fundamental point: not all data brokers work the same, and accordingly, privacy laws do not affect them all in the same way. To effectively regulate them, legislatures must go beyond just taking a macro look at the aggregate effect and further home in on the largest brokers to guarantee the realization of privacy rights where they are needed most. In other words, the simple fact that Cuebiq has so many opt-outs does not indicate that consumers are using the transparency model to knowingly bridge the interaction gap; a larger number of opt-outs, in isolation of the broker's specific privacy policies and data practices, says little

---

169 *Privacy Policy*, CUEBIQ (Nov. 26, 2024), https://perma.cc/TDA6-B562.

170 *Id.*:

> You may limit the disclosure of certain Information by your mobile device to us and mobile app publisher Suppliers by adjusting the settings on your mobile Device. . . . We honor these "limit" or "opt out" instructions or "flags" by removing recognized devices from our cross-app advertising or ad delivery and reporting solutions, on a going forward basis.

171 *U.S. Data Product Privacy Notices*, *supra* note 142.

about the efficacy of the transparency model by itself. While this Comment does not attempt a similarly close examination of every broker in the dataset, the Cuebiq example illustrates that aggregate statistics generally cannot determine that the transparency model works as intended.

4. Consumers prefer to exercise their rights to delete and opt out.

In crafting regulation, it is also important to understand consumer preferences surrounding privacy rights, especially since states have crafted regulations that rely upon consumers exercising control over their data. One way of exploring this is by looking at what types of requests an individual broker receives. They must provide consumers the rights to know, delete, correct, limit, and opt out[172]—but the breakdown between these types should reflect which rights consumers find most valuable to exercise. For all firms reporting a total of one hundred or more requests received, the following five charts present the proportion of total requests for each of the five types.[173]

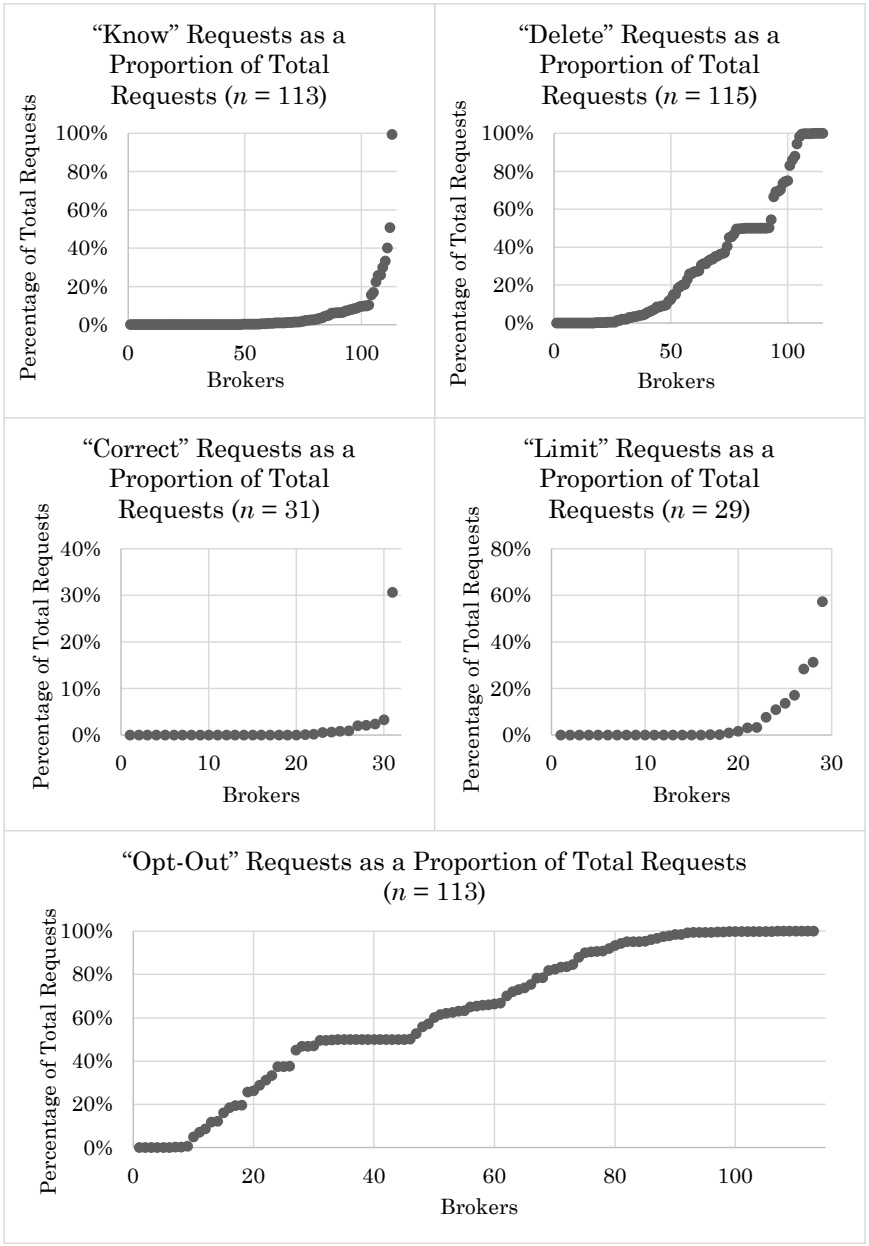
---

[172] Not all data brokers need to provide all rights. For example, they need to provide the "right to limit" only if they have sensitive personal information. *See* CAL. CODE REGS. tit. 11, § 7011(e)(2)(E) (describing how the CCPA confers the right to limit "[i]f the business uses or discloses sensitive personal information"). They need to provide the right to correct only if they store any information themselves. *See id.* at tit. 11, § 7001(dd) (defining the "right to correct" to apply only to information that a business "maintains" about a consumer).

[173] These charts were made as follows: For each California-reporting broker, I determined the total number of consumer privacy requests. This was either taken directly from the privacy policy (if reported) or taken as the sum of all request types. I then filtered to include only those brokers that reported one hundred or more requests. I divided each reported request type by the number of total requests. For example, if a broker reported one hundred total requests and seventeen requests to delete, their delete requests as a percentage of total requests is 17%. After doing this for all brokers and all request types, I assembled these charts. These percentages are plotted on the y-axis, with each dot representing a single broker.

For each chart, I excluded brokers that did not report a number for that request type. For example, many brokers reported the number of received requests to delete but did not report the number of requests to correct. In a case like that, I included the broker on the "delete" chart but excluded it from the "correct" chart.

FIGURE 2: PERCENTAGE OF TOTAL REQUESTS BY REQUEST TYPE



From these charts, I can categorize the five rights into three different groups that exhibit different consumer behavior. The first group includes the least used: requests to know and correct. The second group is somewhere in between: requests to limit. And

the final group includes the ones that are the most interesting because they are the most exercised by consumers: requests to delete and opt out.

First, requests to know and correct make up small proportions of the requests made, and this likely reflects consumer disinterest in exercising those rights, which seems to be a rational response to the unique way in which consumers do not directly interact with brokers nor need to continue using their platforms. This is particularly true for requests to correct, which make up fewer than 5% of the total requests for almost every single broker that reports them.[174] It is still mostly true for requests to know, although they do exhibit a longer tail. This is not surprising. These results are easily aligned with expected consumer interests. Because consumers do not use data broker platforms, they have little reason to care what data is stored or correct any inaccuracies[175]—they likely prefer to just go ahead and either delete it or restrict its usage. In other words, there is no required maintenance of data because they do not need to keep using the platform, so interest in requests to know and correct appears reduced.[176]

Requests to limit fall somewhere in between. These are specifically about limiting the use of sensitive personal information, so firms need to provide the option only if they use such information.[177] It thus makes sense that some brokers who use sensitive personal information would see a higher proportion of limit requests. For example, hireEZ, a talent acquisition platform, has limit requests comprising over 30% of their total volume,[178] which makes sense because their privacy policy explicitly states that they infer "diversity and immigration information,"[179] both of which are sensitive kinds of personal

---

[174] The one exception is LexisNexis, for which correction requests make up over 30% of total privacy requests. Dataset, *supra* note 17.

[175] For example, the value a consumer gets from correcting a broker's mistaken data is usually some marginally improved advertising—which generally will not warrant the effort it takes to exercise the right. This may change if the broker's data affects consumers in a more material way, like in a job application.

[176] Alternatively, it may be that requests to know and correct are less accessible or otherwise more difficult to complete. While this likely does not explain the entire difference, future empirical work could explore this possibility.

[177] This explains the small number of firms reporting numbers for limit requests, and it may also explain why some of the firms report zero limit requests.

[178] Dataset, *supra* note 17.

[179] *General Privacy Policy*, HIREEZ (Mar. 4, 2024), https://perma.cc/T66G-U2ZW.

information.[180] Therefore, the right to limit is an important and effective consumer right, but the domain of application is more limited than the others.

The final category includes the most used and fundamental rights relevant to data brokers: the rights to delete and opt out. As seen in the plots above, these make up a relatively high proportion of all requests. This makes sense for a couple of reasons. First, as described above, consumers do not "use" data broker platforms and thus do not need to keep their data there—they can instead just get rid of it or restrict its use. Second, these requests are the most accessible. Requests to delete might have been forwarded on from actual consumer platforms as required by the CCPA.[181] Requests to opt out might have smaller interaction gaps because opt-out mechanisms are often more directly integrated in consumer-facing applications.[182] In other words, these requests are most likely to close the interaction gap between consumers and brokers themselves.

The following figure more closely examines the relationship between delete and opt-out requests. It plots the ratio between delete and opt-out requests for every California-reporting broker with at least one hundred total requests and more than zero opt-out and delete requests.[183] A number greater than one indicates that there are many more delete than opt-out requests, while a number less than one indicates that there are many more opt-out requests. The median ratio is 0.39 with significant tails.[184]

---

[180] CAL. CIV. CODE § 1798.140(ae).

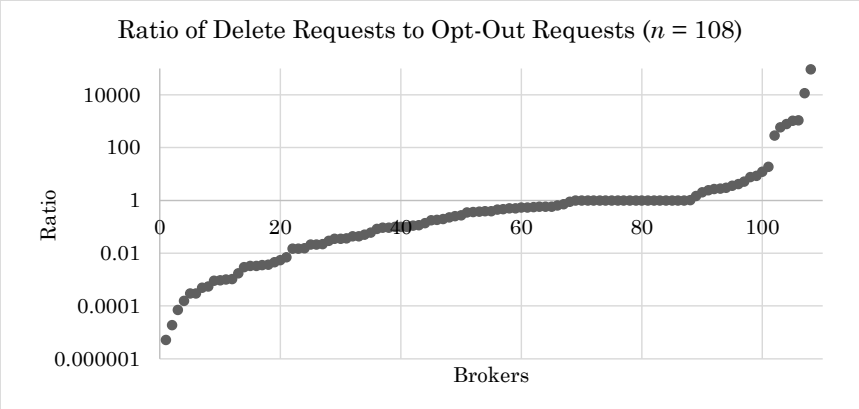
[181] *See supra* text accompanying note 71.

[182] *See also supra* Part III.C.3 (hypothesizing why Cuebiq has so many opt-out requests). Other types of requests, by contrast, are less likely to have these smaller interaction gaps. For instance, while there may be a data-sharing pop-up in iOS apps, there is no automatic data-deleting pop-up.

[183] If a broker had one hundred or more total requests (as reported directly by them or summed from their reported numbers for each request type), the number of delete requests was divided by the number of opt-out requests.

[184] Dataset, *supra* note 17.

FIGURE 3: THE RATIO OF DELETE REQUESTS TO OPT-OUT REQUESTS



The results shown are perplexing, and the only thing evident is that there is no consistent ratio shared across brokers. Generally, brokers receive more opt-out requests than delete requests, but it is not clear why. Consumers do not directly interact with brokers, so if they exercise their privacy rights, we would expect them to go one step further and delete the data rather than just opting out—which is effectively a half measure. The importance of deletion, in particular, gives the Delete Act its name and principal purpose. Positing that consumer preference between deleting and opting out is at most neutral, there must be some alternative mechanism nudging these statistics into a clear preference for opting out. One possible explanation is that the ability to opt out has less of an interaction gap. For example, brokers that are more closely integrated with consumer platforms may be more susceptible to user choices to opt out. Opt-out requests are both preferred by consumers[185] and easier to use[186] in consumer platforms, so a smaller interaction gap would let more opt-out requests bleed through to closely integrated brokers.

The other interesting result in the ratios is the variation. While the difference between the two types of requests is generally within an order of magnitude, there is extreme variation on

---

[185] Corren, *supra* note 69, at 2023 (discussing how opt-out rights are the most used by consumers).

[186] This is because opt-out requests can come from Global Privacy Controls or other platform settings. Also, brokers often directly link to opt-out request forms on their websites' homepages; these opt-out forms do not require the same level of verification that delete requests do.

either end. One broker (Sabio) has over ninety-three thousand times more delete requests,[187] and another (StackAdapt) has over fifty-two thousand times fewer delete requests.[188] Privacy policies rarely explain such disparities. Some of these numbers seem implausible in context: Sabio, for instance, reports over 1.5 million requests to delete but only lists one method to submit deletion requests: an email.[189] It seems unlikely that, in just one year, over 1.5 million people emailed this relatively unknown company. There must be something else at play—such as request forwarding from consumer platforms—that is left unstated in the privacy policy.[190]

All of this indicates that the most frequently exercised rights are the rights to delete and opt out. Many brokers process more opt-out requests, but these numbers do not necessarily reflect consumer preferences. Instead, they more plausibly reveal that opt-out requests are often "easier" to get through to brokers than delete requests. Regulators must be conscious of this effect, both in designing laws and evaluating their effectiveness. For instance, regulation could focus on bolstering consumers' ability to make delete requests—both as a means of reflecting plausible consumer preferences and tailoring mechanisms to close the interaction gap. In fact, this is exactly what California's Delete Act does. And in 2026, we will begin to see the results of such a clear focus as the accessible delete mechanism goes into effect.[191]

5. Many brokers are not significantly impacted by the transparency model of regulation.

The data tells one final story: general privacy rights frameworks, which were designed with consumer interaction in mind, do not work particularly well in facilitating consumers' exercise of their privacy rights for data brokers. This confirms the

---

[187] Sabio reported 1.59 million delete requests and only 17 opt-out requests. Dataset, *supra* note 17.

[188] StackAdapt reported 52,468 opt-out requests and only 1 delete request. *Id.*

[189] *Sabio Inc. Privacy Policy*, SABIO (Aug. 2, 2024), https://perma.cc/EF2G-PE5G.

[190] ShareThis, by contrast, does explain the difference. It is an ad platform that recognizes browser opt-out preference signals. *Privacy*, SHARETHIS (July 3, 2024), https://perma.cc/R44Z-47NX ("You may also stop the collection of your Usage Data by using the do-not-track function, opt-out preference signals, or similar privacy controls of your browser."). Given that ShareThis's website tools embed themselves in other websites, the company would directly respond to these signals from users and likely includes them in its count.

[191] *See supra* text accompanying note 101.

intuitive limits of the transparency model as a form of data broker regulation.

These limits first emerge at a high level when looking at relative data-rights usage rates. While the data presented above may look promising—seven firms, after all, report a total of over one million consumer requests[192]—it paints an incomplete picture. As described, those highest-reporting brokers *are not* the largest brokers and are likely just the ones with the smallest interaction gaps.[193] Consider instead the numbers for the purported largest broker. Acxiom, a platform claiming to have 2.5 billion consumers' data,[194] reported a total of roughly seventy-seven thousand consumer privacy requests from California in 2023.[195] Of those, only about three thousand were delete requests.[196]

This conclusion is affirmed on a second comparison with other consumer-facing firms. Sticking with Acxiom, one can compare it to other large, nonbroker technology companies that have reported their privacy-rights request metrics under the CCPA. PayPal—a company that until recently did not even sell or share data—had over 400,000 delete requests,[197] a figure that is 125 times more than Acxiom. Microsoft had nearly 800,000 delete requests.[198] The difference is not that Acxiom has data on fewer consumers, so it must be that comparatively fewer consumers make requests for Acxiom.

This is particularly notable because we might expect that consumers would, if given the choice, prefer to exercise their rights with brokers. From the consumer's perspective, giving your data to Amazon while directly transacting on Amazon.com makes sense; one may prefer Amazon to possess more information about one's purchase history or street address to facilitate better service going forward. But the same does not apply to brokers. Because consumers do not "use" Acxiom, and because they generally lack transparency into where the data held by Acxiom goes, they should feel more willing to exercise their privacy rights against it. The fact that the data does not bear this intuition out likely

---

192 *See supra* Table 1.

193 *See supra* Part III.C.3.

194 ACXIOM, *supra* note 7, at 2.

195 Dataset, *supra* note 17.

196 *Id.*

197 *California Privacy Rights Reporting*, PAYPAL (June 27, 2024), https://perma.cc/LV69-TR5M.

198 *U.S. State Data Privacy Laws Notice*, MICROSOFT (Sept. 2024), https://perma.cc/5V9Q-TRBB.

indicates the presence of other factors nudging consumers away from exercising their rights and following through on their expected preferences. This could be the interaction gap, or it could be another source of friction, but the effect is notable.

It is important to note, however, that the data is not uniform. As described above, some brokers, like Cuebiq, do receive many requests.[199] And some consumer-facing firms, like Meta, have shockingly few consumer requests.[200] But as long as some brokers have one's data and are willing to sell it to third parties, the floodgates are open. Whether offered by one broker or one hundred, the data is on the market and available to be exploited.[201] In this sense, it is not enough to look at the firms most impacted by the transparency model as a testament to its success; rather, regulators must look to the least impacted because that is the ultimate measure of the actual effect on the data economy. Here, both in aggregate and when compared to consumer-facing firms, very few consumers are exercising their privacy rights against brokers.

IV. RECOMMENDATIONS FOR REGULATORY ACTION

Part III takes a first step toward analyzing this first-of-its-kind data and raises a set of high-level findings. These include that (1) different broker business and technological models lead to different efficacies, likely due to differently sized interaction gaps; (2) consumers most frequently exercise their rights to delete and opt out, suggesting that these are the rights they care most about; and (3) brokers generally do not receive many privacy requests, both when looked at in isolation and when compared to consumer-facing firms. Furthermore, the dataset itself demonstrates that compliance has been difficult, both within California and across states. This all justifies two sets of recommendations, one about lawmaking and another about enforcement.

First, if seeking to truly empower consumers to control their data in the data broker ecosystem, lawmakers need to go beyond

---

[199] *See supra* text accompanying note 167.

[200] Meta reported only 1,193 CCPA requests to delete in 2023, for instance. *California Privacy Rights Report*, FACEBOOK, https://www.facebook.com/legal/policy/ccpa/transparencyreport. This can likely be explained, however, by Meta offering self-serve tools to delete accounts that are not counted as CCPA requests.

[201] This creates a competitive incentive for brokers to avoid compliance as much as possible—another reason why states should be sure to strictly enforce their broker regulations.

the transparency model. This is the extent of the framework currently in effect in California, and the data shows that it is not dramatically affecting most brokers. Many large brokers receive very few privacy requests—particularly compared to comparably sized consumer-facing firms.[202] Some of the brokers that receive many requests only do so because of their business model, not the relevant data broker law.[203] In other words, it seems the transparency model of data broker regulation is not meaningfully affecting the data broker economy. It is not enough to just tell the public who the data brokers are; the law must give them a mechanism to do something about it efficiently and easily to solve the interaction gap.

There are two ways to close the interaction gap. The first is to close the gap between consumer-facing firms and brokers such that requests to consumer-facing firms end up affecting practices of the brokers they sell to. The clearest example of this is the request forwarding mandated for delete requests under California law.[204] The second is to close the gap between consumers and brokers such that a consumer can efficiently make a request to any broker that has their data. This is the innovation at the core of the Delete Act, and it could theoretically be extended to other rights as well.

Different considerations favor the different approaches. Cost favors the first category, namely, leveraging the relationships between consumer-facing firms and brokers. This approach shifts costs to firms: they must close the gap themselves. By contrast, the second category burdens the government, as it is the clearest candidate to build a system like the one described in the Delete Act.[205] Still, consumer interest favors the Delete Act model. The request-forwarding mandate capitalizes on consumers' current usage of their CCPA rights and does not require them to learn about this external, data broker–exclusive mechanism—but it does require them to use their rights against consumer-facing

---

[202] *See supra* Part III.C.3 (discussing how most data brokers, including some large ones, do not receive many consumer privacy requests); *supra* Part III.C.5 (demonstrating that data brokers receive fewer requests than comparatively sized consumer-facing firms).

[203] *See supra* Part III.C.3 (describing how Cuebiq likely has so many requests because of its close integration into data-collecting apps and not because consumers are using data broker registries).

[204] *See supra* text accompanying note 71.

[205] However, the government could fund this development with registration fees or fines collected from enforcement actions.

firms. By contrast, the Delete Act model does not require consumers to exercise their rights against the many different consumer-facing firms they interact with, and instead just requires the submission of a single request. It also opens the possibility of deleting data from brokers who scrape publicly available information.[206] In sum, then, the best path forward is to advocate for the Delete Act model. Ideally, this could be expanded both in scope (across privacy rights) and in jurisdiction (beyond California).

Admittedly, the results are preliminary. While they indicate a deficiency of the transparency model—at least as it worked in 2023 for a certain group of consumers in California—they do not guarantee that the Delete Act model will achieve significantly better results. Thus, additional empirical analysis will be necessary once that Act takes effect. But it is unwise to wait to take regulatory action until 2027, when the Act's results will first be reported.[207] The policy issues around data brokers are pressing; new instances of data misuse are discovered all the time.[208] Whether by adopting the Delete Act model directly or innovating further, regulators should meaningfully empower consumers in reshaping this sector of the economy.

These regulatory systems should further prioritize consumer preferences. My findings demonstrate that consumers likely care the most about exercising their rights to delete and opt out. With limited regulatory bandwidth, legislators should focus their attention on bridging the interaction gap for these specific rights.

Second, regulators need to ramp up enforcement and make guidelines clearer. The findings demonstrate that large numbers of brokers are noncompliant in various ways.[209] This is a clear avenue for enforcers to take action. At the core of this is timely registration, which is an antecedent condition to all other benefits. If brokers do not perceive a real threat of penalization, they may continue to skirt by. Furthermore, the disparities across different state registries[210] provide a clear place to start in enforcement sweeps. Another issue is the lack of clear regulatory guidance. For instance, brokers seemingly have conflicting interpretations of

---

[206] For example, a broker may scrape social media sites or public records. The request-forwarding mandate would not provide a mechanism to delete this data or opt out of its collection because no consumer-facing firm provided it to the broker in the first place.

[207] Because Delete Act–style deletion mechanisms take a long time to build, delaying enactment of a law until 2027 would push its effectiveness even further back.

[208] *See supra* notes 31–33 and accompanying text.

[209] *See supra* Part III.C.1.

[210] *See supra* Part III.C.2.

the metrics provision.[211] This is a simple and straightforward issue to resolve through better official guidance.

One might object to these conclusions on the grounds of the privacy paradox. As discussed, this refers to the observed phenomenon that consumers often do not act in privacy-conscious ways despite expressing pro-privacy preferences.[212] Thus, it might be the case that the transparency model is not missing some uncaptured consumer desire to restrict data brokers—that desire might just not be there in the first place.

I think this objection is misguided for three reasons. First, the data suggests that consumers are often less frequently exercising privacy rights against brokers than they are against comparable consumer-facing firms.[213] This indicates that there are some privacy-conscious individuals acting on such preferences for consumer-facing firms but not brokers, which is counterintuitive to expected preferences. Because consumers see the benefits they get from consumer-facing firms, they should be *more* willing to trade their data for it. The fact that the data suggests the opposite indicates that it is most likely a deficiency of the regulatory model itself. Second, the privacy paradox may take a much different form for data brokers. Because consumers do not directly interact with brokers, they do not knowingly sacrifice anything by enforcing privacy rights against them. Consumer-facing firms, by contrast, might present more immediately apparent negative consequences when a user takes privacy-conscious actions. It is thus unclear whether the privacy paradox maintains the same form in the data broker environment, where consumers are not as readily confronted with the cost of privacy. Third, consumers having slight, but not substantial, preferences points in favor of implementing an efficient mechanism of exercising rights, like the Delete Act does. Such slight preferences are unlikely to justify a consumer spending inordinate amounts of time making privacy requests, so effective regulation would need to make the process minimally time-consuming.

In short, two key takeaways emerge from the data. First, regulators should innovate beyond the transparency model—and perhaps adopt the Delete Act model—to empower consumer privacy against data brokers. Second, regulators must be proactive in enforcement but diligent in guidance. Navigating this

---

211 *See supra* Part III.C.1.

212 *See supra* notes 68–70 and accompanying text.

213 *See supra* Part III.C.5.

increasingly regulated space is new and difficult, and the law should aim to make it easy for both the brokers it is designed to regulate and the consumers it is designed to protect.

CONCLUSION

Having enacted general data privacy statutes, many states are seeking a new frontier in their efforts to reshape the modern data economy to be more consumer conscious. For many, this next frontier appears to be data broker regulation. Some states have taken the first steps to doing this—primarily by prioritizing transparency. The theory is, put simply, that consumers can exercise rights if they know who the data brokers are. California will soon go farther, providing consumers an efficient way to delete their data across all brokers.

This Comment presents a first-of-its-kind methodology and dataset for empirically analyzing the real-world impact of the transparency model on data brokers. It uses this data to argue that transparency is simply not enough. Rather, if seeking to meaningfully effectuate consumer rights and place practical bounds on the data broker economy, governments must provide more efficient tools to close the interaction gap between consumers and brokers. California's recent innovation in the Delete Act is one such example.

More can be done with the dataset presented here. For what types of brokers do consumers prefer to delete their data? Are brokers denying requests? How long do they take to respond? There is an immense amount of useful information—both about what consumers do and what brokers do—that is yet to be extracted from this dataset. I call for researchers to answer these questions and to more fully explore how brokers are affected by consumer privacy frameworks.

All of these questions and more should inform the next wave of regulation. As data brokers grow in economic power and influence, lawmakers seeking to have a meaningful effect must innovate in their attempts to regulate them, and those lawmakers should ground their innovations in empirical understandings of how they actually work. Brokers form a giant sector of the economy and are largely left unconstrained by the traditional limitations of physical commerce or any meaningful government regulation. This free-rein era must end.