Before the
CONSUMER FINANCIAL PROTECTION BUREAU
Washington, D.C. 20580

COMMENTS

of

PRIVACY FOR AMERICA

on the

Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Docket No. CFPB-2023-0020

Counsel:
Stuart P. Ingis
Tara Sugiyama Potashnik
Rob Hartwell
Allaire Monticollo

Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

July 14, 2023

Privacy for America is a coalition of top trade organizations and companies representing a broad cross-section of the American economy, including household brands, media companies, trade associations, advertisers, and more.[1] We appreciate the opportunity to provide comments on the Consumer Financial Protection Bureau's ("CFPB") "Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information" (the "RFI").[2] The collection and transfer of "consumer information" facilitated by "data brokers" makes consumers' access to vital resources, products, services, and information possible, and it fuels a vibrant, thriving economy. Privacy for America strongly supports federal, preemptive consumer privacy legislation to provide privacy protections for individuals across the United States, and we support the CFPB's mission to ensure consumers are treated fairly by banks, lenders, and other financial institutions.[3] However, we strongly believe a federal privacy standard must be enacted by the democratically accountable representatives in Congress. We ask the CFPB to respect the bounds of its statutory authority and refrain from encroaching on areas that should be left to Congress to legislate, as described in more detail in the comments that follow below.

The RFI begins by cataloging a series of events that led to the passage of the Fair Credit Reporting Act ("FCRA") in 1970.[4] The RFI emphasizes principles of transparency regarding personal data use, consumer access to personal data, accuracy in personal data maintained by businesses, and data security.[5] Each of these principles is already reflected in existing requirements for "data brokers" and other businesses under various laws—both federal and state—and is incorporated into many such entities' data practices today. Additionally, when companies run afoul of existing legal requirements, several governmental agencies are authorized to bring enforcement actions to seek redress for violations. Even though companies already embrace the principles articulated in the RFI, build them into the design of their business models, and are subject to enforcement under existing laws, the RFI takes a negative view of data services companies, *i.e.*, "firms that collect, aggregate, resell, license, or otherwise share consumers' personal information with other parties."[6] The RFI generally asserts that consumers and competition suffer a broadly construed conception of "harm" due to actions taken by data services companies, and it asks several questions aimed at creating a record to back this unsupported assertion.

Despite the RFI's focus on perceived "harms" caused by "data brokers" and the collection and sale of "customer information," offerings powered and enabled by data services companies significantly benefit consumers and businesses of all sizes. Data services companies facilitate innovation, driving the proliferation and advancement of better products and services from which consumers derive substantial benefits. Offerings provided by data services companies allow consumers to access more relevant products, content, and services for lower prices—oftentimes for free. Data services companies are also integral to leveling the economic

[1] Privacy for America, *Furthering Accountability and Responsible Data Practices*, https://www.privacyforamerica.com/ (last visited Jul. 14, 2023).
[2] 88 Fed. Reg. 16951-16954 (Mar. 21, 2023) (hereinafter, "RFI"); *see also* 88 Fed. Reg. 38499-38500 (Jun. 13, 2023).
[3] CFPB, https://www.consumerfinance.gov/ (last visited Jul. 14, 2023).
[4] RFI at 16952.
[5] *Id.*
[6] *Id.*

playing field. Small, start-up, and mid-size companies can leverage third-party data to compete on more equal footing with the economy's largest players thanks in part to data services companies.

Any new requirements related to the "collection and sale of customer information" should be legislated by Congress, apply to the entirety of the economy, and not focus only on a narrow set of entities that are data services companies or "data brokers." Our comments proceed by first discussing limitations on the CFPB's authority to issue rules or regulations in this area and by encouraging the agency to respect the bounds of its statutory authority. We then discuss the benefits data services companies provide to consumers and the economy alike, and we describe Privacy for America's *Principles for Privacy Legislation* (the "Framework"), which outlines an effective approach to the creation of a national, preemptive, and comprehensive standard for consumer privacy and data security by Congress.[7] Instead of embarking on an effort to regulate data services companies or limit the collection and use of data about consumers, the CFPB should work with the Congress to help it pass preemptive federal privacy legislation that embraces the standards set forth in the Framework.

I. The CFPB must remain within the bounds of the authority granted to it by Congress when taking any action.

The RFI asks commenters to supply arguments the CFPB can use to support its efforts to take action with respect to data services companies.[8] Federal agency regulatory activity must be traceable to a clear delegation of authority by the Congress. However, the statutes that govern the bounds of the CFPB's authority do not explicitly or implicitly give the agency the power to issue sweeping and encompassing regulations impacting the collection, use, and disclosure of data about consumers by data services companies.[9] The services provided by data services companies that are not subject to the FCRA and the CFPB's authority cannot, absent clear congressional action, be simply "read into" scope, purportedly establishing such an expansion of the CFPB's authority. Moreover, the FCRA is explicitly designed to apply to certain types of data used for particular purposes, specifically consumer reports used for enumerated purposes.[10] Attempts to broaden the reach of the statute to permit regulation of all data types and uses for all data services companies would ignore the unique and specified focus of the FCRA itself. The CFPB should exercise caution in determining next steps after reviewing input in response to the RFI and should decline to embark on overly broad regulatory efforts with respect to data services companies or the collection and sale of "customer data" for purposes outside its clearly delegated authority.

The U.S. Supreme Court has consistently emphasized that Congress must "speak clearly if it wishes to assign to an agency decisions of vast economic and political significance."[11] As recently as 2022, the Supreme Court found that a clear congressional statement is necessary to

---

[7] Privacy for America, *Principles for Privacy Legislation*, https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/ (last visited Jul. 14, 2023) (hereinafter "Framework").
[8] *See* RFI at 16954, *Market-Level Inquiries* at Question 22.
[9] *See* FCRA, 15 U.S.C. § 1681 et seq.
[10] 15 U.S.C. § 1681b(a).
[11] *Utility Air Regulatory Group v. EPA,* 573 U.S. 302, 234 (2014).

delegate broad authority to an agency to regulate a fundamental sector of the economy.[12] In *West Virginia v. EPA,* the Court invalidated regulatory action taken by the Environmental Protection Agency ("EPA"), citing the "major questions doctrine" and deeming the EPA's Clean Power Plan to be an overreach and misinterpretation of its own authority.[13] If the CFPB were to attempt to issue regulations to govern all "collection and sale of consumer data" by data services companies under the FCRA, such regulations would not be traceable to a clear instruction or delegation from the Congress through that federal statute. Neither the FCRA itself nor any other federal statute provides specific authority for the CFPB to regulate such broad areas of the market. Even outside of the FCRA context, the CFPB's authority to regulate is limited to consumer financial products and services; the agency has no authority to regulate data services companies writ large. Products provided by data services companies impact all consumers and touch virtually every vertical of the economy. Consequently, regulations inhibiting the collection or sale of "customer data" would pose a major question that, pursuant to separation of powers principles, would require Congress to determine via legislation.

Despite the limits of the FCRA and other related statutes, the CFPB has taken several actions with the aim of expanding its own authority. Through interpretive rules, advisory opinions, and, most recently, a procedural rule, the agency has indicated an intent to exercise a "dormant authority" to exercise supervisory authority over nonbanks.[14] In a 2014 report, the FTC called for new legislation to govern data services companies, thereby acknowledging and affirming that, in the FTC's consideration of the industry, neither it nor the CFPB had existing regulatory authority over such companies when they engage in activity outside the scope of the FCRA.[15] Attempts to bootstrap or expand an agency's regulatory authority by leveraging equivocal or imprecise provisions in legislation are very likely unconstitutional.[16] The CFPB must remain within the bounds of the power delegated to it by Congress, and its response to the RFI should take into account the existing and clear limitations on its authority.

---

[12] *West Virginia v. EPA*, 142 S. Ct. 2587. (2022).
[13] *Id.*
[14] *See* CFPB, *CFPB Invokes Dormant Authority to Examine Nonbank Companies Posing Risks to Consumers* (Apr. 25, 2022), located here.
[15] *See* FEDERAL TRADE COMMISSION, *Data Brokers: A Call for Transparency and* Accountability at 49-54; 51 n.86 (May 2014), located here (hereinafter, "FTC Report'); *see also* SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS MAJORITY STAFF, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* at 8 (Dec. 18, 2013), located here; *see also* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Statement of Alicia Puente Cackley, Director Financial Markets and Community Investment* before the *Senate Committee on Banking, Housing, and Urban Affairs*, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps* at 7, 12-13 (Jun. 11, 2019), located here; *see also* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Report to the Chairman, Senate Committee on Commerce, Science, and Transportation, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* at 31-34 (Sept. 2013), located here.
[16] *See generally West Virginia v. EPA*, 142 S. Ct. 2587 (2022).

II. Consumers benefit significantly from the collection and use of data facilitated by data services companies.

While several questions in the RFI ask for information about purported "harms" associated with data services companies,[17] very few questions ask commenters to supply information about the benefits data services companies offer to consumers and the economy. One question asks, generally, "[w]hat data broker practices provide benefits to people? [And w]hat are those benefits?"[18] Data services companies help businesses of all sizes innovate and improve their products and services, which ultimately yields better results for consumers to enjoy a larger universe of products and services. With respect to the financial sector in particular, data services companies provide anti-fraud and identity theft monitoring products, which enable consumers' access to a variety of companies with which they can transact, and data services companies help facilitate greater access to financial instruments.

Without information from data services companies, it would be much more difficult for companies to verify consumer identities, detect and deter fraud, and limit negative outcomes from stolen or misappropriated information.[19] A lender, for instance, could use a data services company's identity verification products to confirm that a person presenting herself as "Mary Smith" with a physical home address of 100 Main Street is, in fact, the person they say they are. That same lender may use an anti-fraud product or an identity detection service to pin flags to names or accounts if a Social Security number provided as part of a loan application process has recently been used in conjunction with several different physical addresses, thereby suggesting fraud attempts may be present. Data services companies power these important identity monitoring and anti-fraud services that provide robust consumer protection against identity theft.

Data services companies also provide third-party data sets to the marketplace that help subsidize the cost of the offerings businesses provide to consumers. These third-party data sets, for instance, subsidize the vast and varied free and low-cost information, products, services, content, and resources consumers can access online today. Because businesses can collect and transfer data and reach consumers at a lesser cost by leveraging third-party data provided by data services companies, businesses can afford to offer many of their products, services, and content at a low fee or for free. One study found that the ad-supported Internet, powered by third-party data sets and data services companies, provides at least 30,000 dollars of value to individual consumers per year, measured in 2017 dollars.[20] Because the United States' population amounts to well over 300 million individuals, this figure suggests that laws or regulations threatening third party data sets and data services companies' ability to remain viable could have trillions of dollars of impact on consumers holistically throughout the U.S. economy.

Without data services companies, or in an environment where data services companies are subject to unreasonable restrictions, many offerings and content found online today would be

---

[17] See RFI at 16953, *Market-Level Inquiries* at Question 2b; RFI at 16954, *Market-Level Inquiries* at Question 13a, 13b, 13c; *RFI* at 16954, *Individual Inquiries*.
[18] *See* RFI at 16954, *Market-Level Inquiries* at Question 14.
[19] *See* FTC Report at 32-33.
[20] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data* at 16 (Nov. 2022), located here (hereinafter, "Beales & Stivers").

much more expensive to provide, and this reality could push businesses to lock their information behind paywalls. This shift in the status quo of today, where much online information and content is largely free or provided at a low cost, would negatively and disproportionately impact consumers with less expendable income in comparison to those who have significant excess income to be able to pay for access to Internet resources on a site-by-site basis. Data services companies thus help democratize access to the Internet by helping to create an environment where information, products, and services are widely accessible by all individuals. Data services companies help ensure consumers of all economic echelons can reach critical information and resources for free or at a low cost.

Under current laws, regulations, and industry self-regulatory programs, data services companies, like other businesses in the marketplace, are required to provide robust transparency regarding their use and transfer of personal data and observe consumer choice and controls with respect to certain data processing activities. For example, data services companies that engage in or support online behavioral advertising are subject to the notice and opt-out requirements of the Digital Advertising Alliance's ("DAA") Self-Regulatory Principles (the "Principles").[21] The core tenets of notice and choice under the Principles have been extended to the multi-site, mobile, and cross-device environment,[22] and covered data services companies are required to abide by their terms. DAA obligations apply broadly in the marketplace to any entity that engages in online behavioral advertising. Consumers are thus already empowered to learn about ways data services companies use personal data and to opt out of certain processing, uses, and transfers of personal data about them if such uses are of concern to the consumer.

III. Businesses of all sizes rely on data services companies to compete.

The RFI asks commenters to supply information about ways data services companies impact competition in the marketplace.[23] Data services companies, and the third-party data sets they supply, serve a vital role in preserving and enhancing healthy competition in the economy. Third-party data and data services companies help businesses efficiently reach existing customers, find new customers, and develop new markets for their offerings. Without the information and services provided by data services companies, businesses would be limited to using the first-party data sets they maintain to conduct outreach and advertising for their products and services, which is inherently limited to existing customers, or they would be forced to rely on a handful of large platforms to reach target markets. Neither result would support a healthy, competitive marketplace.

Limitations on access to third-party data would reduce companies' ability to reach new customers who may be interested in their products. In particular, the information provided by data services companies is vital to competition and small business viability. Large companies with existing and well-established pools of customers have an advantage in comparison to small, mid-size, and start-up entities that do not have similar access to first-party data and interactions.

---

[21] DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (Jul. 2009), located here.
[22] DAA, Self-Regulatory Principles for Multi-Site Data (Nov. 2011), located here; DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013), located here; DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015), located here.
[23] *See* RFI at 16953, *Market-Level Inquiries* at Question 8.

One study found that "[o]verly broad and rigid restrictions intended to protect privacy," such as those under Europe's General Data Protection Regulation, can reduce funding for innovative new technology companies and start-ups.[24] Start-ups, for instance, cannot effectively reach a target market for their new offerings without the use of third-party data. Since start-up companies do not have their own first-party data sets when they are beginning their businesses, data services companies play a crucial role in their ability to build a brand and a loyal customer base. As a result, data from third parties, such as data services companies, is a vital input that enables small, mid-size, and start-up businesses to compete. Data services companies help small businesses that have less resources than their larger counterparts increase their ability to reach potential customers. Data services companies also help small businesses tailor their products to specific needs of their customers and develop personalized connections with their customers.

Limitations on data services companies or limitations on the availability of third-party data sets would also force companies to depend on just one or two large platforms to disseminate their messages and advertising. This result would create consolidation in the economy and give large platforms undue market power by entrenching them as indispensable intermediaries businesses would *have* to work through to find new customers for their offerings. Data services companies and third-party data sets provide an important check against the potential for the accretion of this excessive power, enabling businesses of all sizes to conduct their own advertising without reliance on large platforms. Data services companies consequently make the economy more efficient and effective, helping to enable a vibrant and healthy ecosystem of competition amongst firms. In particular, studies show that restrictions on the use of third party data "increase concentration" in the marketplace, "fortify" the already dominant positions of incumbent platforms, and encourage the creation of "content fortresses" at the expense of consumers and small and new businesses.[25] Another study found that "a week after GDPR implementation, market concentration increased by 17 percent,"[26] suggesting that onerous restrictions on third party data detrimentally impact the ability of small and new businesses to remain active participants in the economy.

One survey of small businesses showed that the vast majority—approximately 92%—of those companies use data-driven digital advertising, which is powered by data services companies and third-party data sets, while only 39% use traditional advertising methods such as print media, mail, telephone, TV and radio to reach new customers.[27] In 2020, small businesses spent an average 88% of their marketing budgets on data-driven online advertisements, demonstrating the value that personalized digital ads that leverage third-party data and data services companies provide to the small business ecosystem.[28] The same study reported that 72% of small businesses surveyed said data-driven advertising, fueled by data services companies, is "important" to the success of their business.[29] Data-driven advertisements are dependent on third-party data sets and are personalized to individual consumers. Contextual

[24] Beales & Stivers at 3.
[25] *Id.*
[26] Aryamala Prasad, *Two Years Later: A Look at the Unintended Consequences of GDPR*, GEORGE WASHINGTON UNIVERSITY REGULATORY STUDIES CENTER (Sept. 2, 2020), located here.
[27] *See* DELOITTE, DYNAMIC MARKETS: UNLOCKING SMALL BUSINESS INNOVATION AND GROWTH THROUGH THE RISE OF THE PERSONALIZED ECONOMY at 11-12 (May 2021), located here.
[28] *Id.* at 12.
[29] *Id.*

advertising, while valuable, cannot and does not serve as a viable substitute to the value created by data-driven advertising, powered by third-party data and data services companies, as demonstrated by research.[30] One study found that a combination of contextual and behavioral data from third parties performed almost three times better than contextual data alone.[31] In fact, studies also show that primary reliance on contextual advertising advantages large and well-established publishers and brands over small businesses.[32] Onerous or restrictive limitations on data services companies or third-party data sets would consequently entrench large market players and threaten small businesses' viability, which ultimately harms consumers and the economy overall.

IV. Comprehensive privacy legislation, reflective of the principles set forth in the Privacy for America Framework and applied to all entities in the marketplace, is the best path forward to protect consumers and preserve healthy economic competition.

To enhance the strong protections that sectoral laws like the FCRA and others already provide, economy-wide standards for businesses' use and disclosure of data about consumers should apply across the marketplace and should be set by Congress rather than federal agencies. Congress should set such standards for personal data use and disclosure through a comprehensive, preemptive legislative vehicle that clearly defines the contours of permissible data use. To provide the most robust consumer protection and to help ensure that any new requirements do not have unintended anticompetitive effects, privacy legislation should take a holistic approach rather than focusing too acutely on one type of entity in the marketplace.

Privacy for America supports such a comprehensive, preemptive federal solution set by Congress, as described in the Framework. Relevant to the Commission's RFC, Privacy for America's Framework calls for flexible data security standards that are responsive to the nature and scope of the entity implementing the requirement, as well as the sensitivity and risks to the consumer of the personal information being processed.[33] Privacy for America's Framework would also prohibit companies from obtaining a range of sensitive information, including certain financial information, without first procuring consumers' express consent, and would strictly ban the use of personal data to make eligibility decisions about jobs, credit, insurance, healthcare, education, financial aid, or housing outside of the scope of existing sectoral laws, such as the FCRA.[34] The Framework would also provide new tools to regulators to limit suppliers of data that would undermine protections related to uses of data for eligibility purposes.[35] The Framework represents a useful approach for legislators to look to when drafting comprehensive, preemptive privacy legislation, as the Framework clearly defines permissible and prohibited uses of personal information for all kinds of companies—including data services companies.[36]

---

[30] Beales & Stivers, 13-15.
[31] *Id.* at 3, 14, 18.
[32] *Id.* at 11-12.
[33] Framework at Part I, Section III(N).
[34] *Id.* at Part I, Section III(A), H.
[35] *Id.* at Part I, Section III(A).
[36] *Id.* at Part I.

The CFPB should not take any action to attempt to impose limitations on all aspects of data services companies or the third-party data they provide. Instead, the CFPB should observe the statutory bounds of its authority and support the congressional enactment of comprehensive, preemptive data privacy standards that align with the standards set forth in Privacy for America's Framework. As described in these comments, data services companies provide significant value to consumers, competition, and the economy-at-large, and the elected representatives of Congress are best suited to enact across-the-board standards for the use and disclosure of consumer data.

* * *

Thank you for the opportunity to provide comments on the RFI. Please contact Stu Ingis, Counsel to Privacy for America, at singis@venable.com with questions regarding this submission.

Sincerely,

Privacy for America