Comments of Consumer Reports
In Response to the
Consumer Financial Protection Bureau
Notice of Proposed Rulemaking
Protecting Americans from Harmful Data Broker Practices (Regulation V)

By

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

April 2, 2025

Consumer Reports[1] appreciates the opportunity to provide feedback on the Consumer Financial Protection Bureau's (CFPB) Request for Comment on its Notice of Proposed Rulemaking (NPRM) on Protecting Americans from Harmful Data Broker Practices (Regulation V). We thank the Bureau for initiating this proceeding and for its other efforts to provide strong consumer protections in the marketplace.

Consumer Reports previously filed comments in response to the Bureau's Request for Information (RFI) on this docket, detailing the experiences of consumers with data brokers.[2] Consumers reported having difficulty removing information from data brokers' repositories, unsuccessful efforts to opt out of data collection, and a range of harms associated with the collection and dissemination of their information, such as spam, identity theft, fraud, and scams.

In these comments, Consumer Reports largely supports the intent of the Bureau's proposal to bring data brokers under the auspices of the Fair Credit Reporting Act (FCRA). We support amending the definition of consumer reporting agency (CRA) and consumer report to ensure that data brokers that sell information about consumers' credit history or other financial information are CRAs. We also support the proposal to amend FCRA such that CRAs remain covered when they share credit header data with third-parties. However, we note that, without clarification, the Proposed Rule may inadvertently weaken protections for consumers in certain states by allowing data brokers to rely on exemptions in those laws when they include protections that exceed those in FCRA. We provide CFPB with recommendations to mitigate these concerns.

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] Consumer Reports, Response to Request for Information Regarding Data Brokers and Other Business Practices, (July 13, 2023) https://advocacy.consumerreports.org/wp-content/uploads/2023/08/Consumer-Reports-Comment-Letter-on-Data-Brokers.pdf

I. Introduction

As was thoroughly evidenced in the Bureau's commentary in the Request for Information,[3] NPRM,[4] Consumer Reports' previous comments to the Bureau,[5] and in various comments responsive to the RFI,[6] the data broker business model presents a number of significant risks to consumers.

Data brokerage is a multi-billion-dollar industry centered on collecting and selling people's personal data, typically without their knowledge or explicit consent. Data brokers amass personal dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior online and offline, religious practices and beliefs, physical and mental health conditions, finances, political affiliations, precise geolocation derived from cellphones and connected devices, as well as their inferences about individuals based on this existing data.[7] Some data brokers even collect and sell information about children.[8] This information is then sold and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process.[9]

A non-exhaustive list of data broker-driven harms includes:

---

[3] Consumer Financial Protection Bureau, Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Section II, (March 21, 2023), https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection

[4] Consumer Financial Protection Bureau, Notice of Proposed Rulemaking, Protecting Americans from Harmful Data Broker Practices (Regulation V) (henceforth CFPB Proposed Rule on Data Brokers or Proposed Rule), Section II, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[5] Consumer Reports, *supra* note 3.

[6] See, e.g., Electronic Privacy Information Center, Comments on CFPB's Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Section II, (March 21, 2023), https://www.regulations.gov/comment/CFPB-2023-0020-3980; Comment from U.S. Public Interest Research Group and Center for Digital Democracy, (March 21, 2023), https://www.regulations.gov/comment/CFPB-2023-0020-3412

[7] See, e.g., Joseph Cox, The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15, 404 Media (Aug. 22, 2023), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/;
Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Wash. Post (Jun. 24, 2019). https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-how-states-are-trying-stop-them/.

[8] Suzanne Smalley, The Record, "Dozens of data brokers disclose selling reproductive healthcare info, precise geolocation and data belonging to minors," (March 8, 2024), https://therecord.media/dozens-of-data-brokers-disclose-selling-info-on-kids-geolocation-data-reproductive-health

[9] Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 15-16 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use data brokers to target vulnerable individuals for scams, or otherwise use personal information to cause harm. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It," "Retiring on Empty: Single," and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products.[10] Data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[11]

- *Predatory use of consumer data.* Data brokers sell data about people who rarely even know these companies even exist—and who have rarely ever affirmatively, expressly consented to this data collection and sale. In some instances, this can result in financially disastrous consequences for consumers. A recent case brought by the Texas Attorney General alleged that Arity, a data broker owned by the insurance company Allstate, secretly harvested information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[12] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Enhanced risks of data breaches.* Data brokers collect trillions of data points on Americans, so they are unsurprisingly a top target for hackers and cyber criminals. Recently, National Public Data, a data broker that specializes in online background checks and fraud prevention services, saw its own data breached, compromising the privacy and security of 2.9 billion consumers whose personal information they trade in, with particular concern for the 170 million individuals across the US, U.K. and Canada whose sensitive information, including social security number, was exposed.[13] And location data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day,[14] reportedly suffered

---

[10] CFPB Proposed Rule on Data Brokers, Section IV, p. 38, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[11] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs

[12] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

[13] National Public Data breach: What you need to know, (January 31, 2025), https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535

[14] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

a massive data breach that may have leaked the location data of millions of individuals.[15] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[16]

Because of these risks, Consumer Reports has aggressively advocated for greater regulations over the data broker marketplace in a wide variety of contexts. CR has lobbied state legislatures to pass comprehensive privacy laws that include basic procedural rights that allow consumers to exercise control over their personal information collected by businesses, including data brokers.[17] We've also fought for privacy laws to include the concept of data minimization, which would prevent companies from collecting or sharing consumers' personal data unless it is reasonably necessary to provide the requested service — a protection that would substantially limit data brokers' ability to amass consumer data files without their knowledge.[18]

When those measures haven't gone far enough to allow consumers to easily remove their data from data brokers, we have supported data broker sector-specific legislation and regulations to supplement those laws, such as the California Delete Act and associated rulemakings.[19] And we've developed consumer-friendly privacy tools that take advantage of certain provisions in state privacy laws — like the authorized agent provision — that permit authorized third-parties to help consumers manage the cumbersome process of submitting individual opt-out and deletion requests.[20]

We appreciate that with this rulemaking the CFPB is likewise attempting to mitigate harm to consumers by putting meaningful constraints on how data brokers can collect and use personal data. We discuss several aspects of the Proposed Rule in further detail below.

II. Bringing Data Brokers under the Fair Credit Reporting Act

In Section II of the Proposed Rule, the CFPB lays out how data brokers have attempted to evade coverage under FCRA by claiming that they do not "collect, assemble, evaluate or sell"

---

[15] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

[16] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf

[17] See, e.g., Consumer Reports Supports Michigan S.B. 659, Consumer Privacy Legislation, (December 4, 2024), https://advocacy.consumerreports.org/research/consumer-reports-supports-michigan-s-b-659-consumer-privacy-legislation/

[18] Consumer Reports and EPIC Model State Privacy Bill, Section 6, https://advocacy.consumerreports.org/wp-content/uploads/2024/09/EPIC_CR-CT-CLEAN-FINAL-1.pdf

[19] Consumer Reports Supports S.B. 362, the Delete Act, (August 11, 2023), https://advocacy.consumerreports.org/research/consumer-reports-supports-s-b-362-the-delete-act/

[20] Kaveh Waddell, Consumer Reports, "How to Take Back Control of Online Data With Apps Like Consumer Reports' Permission Slip," (October 3, 2023), https://www.consumerreports.org/electronics/privacy/take-control-of-online-data-with-apps-a5151057853/

the same information as other consumer reporting agencies or by claiming ignorance that data they share "is used or expected to be used" for the purposes of establishing eligibility for credit, employment, or other FCRA-authorized purposes. CFPB proposes amending the definition of the key terms "consumer reporting agency" and "consumer report" to clarify that data brokers can no longer rely on these arguments to claim they are exempt from complying with the law.

The Bureau would accomplish this by interpreting the phrase "assembling or evaluating", which appears in the definition of "consumer reporting agency." [21] The proposed change would clarify that a person assembles or evaluates consumer credit information or other information about consumers when they meet one of several criteria, including collecting or retaining such information, assessing the value of such information, or altering the content of such information.[22]

Consumer Reports supports these changes — data brokers that collect and sell the same information as entities acting as consumer reporting agencies or that share consumer information that is then used to make important credit-related decisions should be covered by FCRA. For too long, data brokers have hid behind claims that they are primarily in the business of "marketing" or "risk assessment," when in fact there can be a large degree of cross-over between their activities and the activities of the more traditional credit reporting agencies.

Ultimately, many data brokers employ algorithmic scoring tools or make inferences about individuals that can be used as an input for decisions that impact critical elements of their lives, especially relating to their finances or employment. For example, data brokers may categorize individuals into audience segments — with descriptive categories about individuals' personality traits, level of income, or employment status — that may contain a high degree of valence for those seeking to make these types of decisions. At the same time, the quality of this information is often questionable at best. In one recent study, data brokers only correctly predicted an individual's gender 26.5% of the time — performing far worse than the benchmark of simply guessing.[23] Landlords,[24] financial institutions,[25] and insurance companies[26] have all explored the use of this type of non-traditional information to help them make eligibility determinations. And

---

[21] Proposed Rule, Section 1022.5(b), https://docs.google.com/document/d/1x1VArCtCfasubtFhdqL41_-d5T8_3pD6fEUyWM5Pt-Y/edit?tab=t.0
[22] Ibid.
[23] Nico Neumann, Catherine E. Tucker, and Timothy Whitfield, "Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies," Marketing Science, Vol. 38, No. 6, (October 2, 2019), https://pubsonline.informs.org/doi/10.1287/mksc.2019.1188
[24] TechEquity, "The Promise and Perils of Residential Proptech," (April 2023), https://techequity.us/wp-content/uploads/2023/04/TBHI-Y1-Research-Summary-Report.pdf
[25] Congressional Research Service, "Alternative Data in Financial Services," (November 7, 2024), https://www.congress.gov/crs-product/IF11630
[26] Marshall Allen, ProPublica, "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates," (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

even when data brokers don't directly disclose personal information to these types of entities, it can still make it into their hands via downstream third-parties.[27]

We recognize that some data flows are essential to the functioning of the financial system — such as fraud detection, underwriting, and credit reporting for permissible purposes. However, these activities must be transparent, accountable, and subject to consumer protections. By clearly delineating which data uses are permissible under FCRA and subject to appropriate oversight, the Bureau can preserve legitimate uses while prohibiting exploitative or unaccountable practices.

Consumers deserve the baseline protections in FCRA to ensure that they know when data about them is used for important financial decisions, that the data are accurate, and that they have the ability to correct or delete it when it is not.

III. Communication of Credit Header Data Constitutes a Consumer Report

The CFPB proposes clarifying that the definition of "consumer report" includes the communication of personal identifiers that bear on a consumer's "creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and that are used or are expected to be used as a factor for establishing eligibility for credit, employment, or other FCRA-authorized purposes.[28] Personal identifiers under the Proposed Rule would include name, age, date of birth, addresses, phone numbers, email addresses, social security number, or any other personal identifier for the consumer similar to those listed.

This would close a well-known loophole for "credit header data" that has been exploited by CRAs to sell or share consumer information outside the bounds of FCRA.[29] The loophole allows CRAs to share personal identifiers of consumers that have not been vetted for accuracy in the same way as data in the underlying consumer report, but could nevertheless be used to make eligibility decisions. Furthermore, the Bureau discusses how the sale of credit header data has contributed to harms to consumers, like doxing, fraud, and identity theft.[30] Credit header data

---

[27] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," at 73-74, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[28] Proposed Rule, Section 1022.4(d), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[29] Drew Harwell, Washington Post, "ICE investigators used a private utility database covering millions to pursue immigration violations," (February 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/

[30] CFPB Proposed Rule on Data Brokers, Section IV, Proposed § 1022.4(d) Would Promote the FCRA's Goals and Prevent Misuse of Personal Identifiers, p. 58, https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

has also been shared with third-parties for non-permissible FCRA purposes, such as marketing.[31]

The Bureau correctly points out that personal identifiers de-facto bear on the "personal characteristics" of consumers and can bear on consumers' creditworthiness, mode of living, or general reputation.[32] The advancement in data processing capabilities since the passage of the FCRA has diminished the distinction between the data in consumer reports and credit header data. Data brokers can use credit header data, especially when combined with other sources of personal information they may collect (e.g. payment information, geolocation, etc.), to make inferences about consumers' financial situations, employment status, and other personal characteristics that would be directly relevant to those seeking to make eligibility decisions.

Even on their own, some personal identifiers are incredibly sensitive pieces of information that deserve heightened protections from credit reporting agencies. There should not be an unregulated market for the sale of consumers' social security numbers and home addresses,[33] full-stop. Considering that in most cases consumers had very little ability to prevent the collection of this information in the first place, they deserve, at a minimum, the ability to access it, and correct and delete it when it is incorrect or incomplete.

IV. Potential Conflict with State Laws

Though we support CFPB's general intent to provide more guardrails for data brokers by bringing them under FCRA, we are concerned that the Proposed Rule will remove some protections for consumers living in certain states that have already passed privacy laws that apply to data brokers. For many data broker records, the CFPB will effectively be substituting strict purpose limitation obligations for existing state rights that consumers have to delete data broker records in their entirety. We recommend that the CFPB clarify the scope of the rule's application to non-financial data broker records that are eventually used for FCRA purposes to ensure that data brokers cannot claim exemption from state privacy laws while avoiding comprehensive compliance with FCRA obligations.

In recent years, a handful of states have passed comprehensive privacy laws aimed at providing consumers with a baseline set of rights intended to allow them to exercise greater control over their personal information collected by covered businesses, including data brokers.[34] Though these laws vary in strength, all of them include the right to know, the right to delete, and the right

---

[31] Ibid, at 16. https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf
[32] Ibid, at 52-53.
[33] While property records may be publicly accessible in many jurisdictions, renters' home addresses are generally not available.
[34] IAPP, US State Privacy Legislation Tracker 2025, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

to access personal data.[35] Most laws also include the right to correct and the right to opt-out of processing of personal data for certain uses.[36]

While some of these rights are roughly analogous with protections in FCRA (right to know, right to correct), some state laws provide protections that exceed those in FCRA. For example, while the FCRA right to delete generally only applies in cases where a consumer asserts that information in their file is incomplete or inaccurate,[37] most state privacy laws allow consumers to delete information with only limited exceptions. Additionally, states are increasingly looking to augment their privacy laws with data broker specific legislation. In 2023, California passed the Delete Act, which builds on the state's existing data broker registry to provide consumers a one-stop-shop to delete their personal information from all of the state's registered data brokers in a single click.[38] Other states are actively considering legislation to mirror the Delete Act.[39]

States are also increasingly including provisions in privacy legislation that would prevent the collection and sharing of personal information not necessary to provide the service requested by consumers (i.e. data minimization) or that would ban the sale of certain classes of personal data (e.g. sensitive data) outright.[40] The data minimization standard would make the practice of data brokerage much more difficult — potentially even impossible — because most data brokers do not have a first-party relationship with consumers and consumers generally do not "request" data broker services. Maryland recently passed a comprehensive privacy law that includes both of these provisions.[41]

At the same time, we recognize that FCRA goes further than many state privacy laws in various ways. For example, coverage under FCRA is not subject to a threshold,[42] while all state privacy laws include some threshold (typically a certain number of consumer records collected in a calendar year, revenue, or other federal guidelines) that could exempt smaller data brokers.[43] If the Bureau's proposal were to be finalized, smaller data brokers could not claim such an exemption.

---

[35] Ibid.
[36] Ibid.
[37] Fair Credit Reporting Act, Section 611 (a)(1)(A), https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf
[38] California S.B. 362, the Delete Act, Section 6, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362
[39] Nebraska LB 602, https://nebraskalegislature.gov/bills/view_bill.php?DocumentID=59563; Illinois HB 2913, https://ilga.gov/legislation/fulltext.asp?DocName=10400HB2913&GA=104&SessionId=114&DocTypeId=HB&LegID=161116&DocNum=2913&GAID=18&SpecSess=&Session=&print=true
[40] See, e.g., Massachusetts H. 78, https://malegislature.gov/Bills/194/H78; Vermont H. 208, https://legislature.vermont.gov/bill/status/2026/H.208
[41] S.B. 541/H.B. 567, the Maryland Online Data Privacy Act of 2024, Section 14–4607(A)(2) and Section 14–4607(B)(1), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0541?ys=2024RS
[42] Fair Credit Reporting Act, Section 603(f), https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf
[43] SourcePoint, The Always-Up-To-Date US State Privacy Law Comparison Chart, (July 1, 2024), https://sourcepoint.com/blog/us-state-privacy-laws-comparison-chart/

Another critical way FCRA (especially under the Proposed Rule) exceeds state privacy protections is in the "permissible purposes" limitations. Under FCRA, a CRA may only furnish a consumer report under certain conditions, such as when the CRA has reason to believe the information will be used in connection with credit transactions or for employment purposes. The Proposed Rule would take this even further by clarifying that the "legitimate business need" permissible purpose does not include furnishing consumer reports for marketing.[44] If the Rule were to be finalized with this provision intact, it would have the potential to drastically cut down on the collection and onward flow of consumer data to hugely pro-privacy effect.

As the Bureau is aware, all of the 19 comprehensive state privacy laws exempt from coverage activities relating to personal information already regulated by FCRA.[45] Therefore, the Bureau's proposal to bring data brokers under FCRA could have the consequence of allowing some data brokers to claim a blanket exclusion from coverage under existing state privacy laws — potentially causing consumers to lose protections that go beyond FCRA, disincentivizing states to continue to iterate on data broker regulations, or incentivizing entities to classify themselves as data brokers to evade stronger state requirements.

As discussed above, we support the Bureau's proposal to ensure that the communication of credit header data is considered a consumer report, subject to FCRA. However, the Bureau's proposed interpretation of the "is used" standard leaves some ambiguity about the breadth of this proposed expansion — and therefore data brokers' ability to leverage state-level FCRA exemptions. The Bureau seeks to classify the communication of any information (including personal identifiers like name, address, age, telephone numbers or social security number) as a consumer report so long as the information "is used or expected to be used" for the purposes of establishing eligibility for credit or other FCRA purposes. The Bureau further explains that the "is used" standard is meant to apply "irrespective of whether the person furnishing the report could have reasonably expected that use or took steps to prevent it."[46] Practically, this may mean that many data brokers will simply treat *all* of the personal information they hold as exempted from state privacy laws if it could theoretically be used by downstream recipients for FCRA related purposes.

While it is unclear whether that outcome is the intent of the Bureau, we note that the proposed framework may incentivize data brokers to claim blanket exemptions in cases where state privacy laws provide consumer protections and rights that go beyond FCRA. For example, data

---

[44] CFPB Proposed Rule on Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Section 1022.12(b)(3), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[45] CFPB, "State Consumer Privacy Laws and the Monetization of Consumer Financial Data," (p. 17), (November 2024), https://files.consumerfinance.gov/f/documents/cfpb_state-privacy-laws-report_2024-11.pdf

[46] CFPB Proposed Rule on Protecting Americans from Harmful Data Broker Practices (Regulation V), Section IV, p. 27, https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

brokers may claim that marketing databases that were previously subject to universal deletion rights under laws like the Delete Act are now FCRA-covered data and therefore out-of-scope — and may even argue that they do not need to comply with FCRA's additional protections until they become aware of use for FCRA purposes.

To avoid ambiguity and prevent data brokers from improperly asserting FCRA preemption, the CFPB should explicitly state in the final rule or its commentary that this rule does not expand the scope of federal preemption under the FCRA. We urge the CFPB to affirm that the final rule does not preclude states from enforcing stronger consumer protections, including rights to delete or minimize data that fall outside of FCRA-covered purposes. The CFPB should also clarify that its proposal does not permit data brokers to simply claim that all their records are exempt from the application of state privacy laws simply because they could potentially be used for FCRA-covered purposes. This would align with the CFPB's previous interpretive guidance that: "...State laws that are not 'inconsistent' with the FCRA—including State laws that are more protective of consumers than the FCRA—are generally not preempted."[47] Such clarification will help ensure that the rule strengthens rather than undermines the broader ecosystem of consumer privacy protections.

V. Conclusion

We thank the CFPB for its consideration of these points, and for its work to secure strong protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.

[47] CFPB, Interpretive Rule, The Fair Credit Reporting Act's Limited Preemption of State Laws, (Section I), https://www.federalregister.gov/documents/2022/07/11/2022-14150/the-fair-credit-reporting-acts-limited-preemption-of-state-laws