COMMENT OF

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")

AND

FIGHT FOR THE FUTURE

BEFORE THE CONSUMER FINANCIAL PROTECTION BUREAU

ON A REQUEST FOR INFORMATION REGARDING DATA BROKERS AND OTHER BUSINESS PRACTICES INVOLVING THE COLLECTION AND SALE OF CONSUMER INFORMATION

SUBMITTED JULY 13, 2023

I. Introduction

The Surveillance Technology Oversight Project (S.T.O.P.) is a community-based civil rights group that advocates and litigates against discriminatory surveillance. Our work highlights the impact of surveillance on Muslims, immigrants, the LGBTQ+ community, Indigenous peoples, and communities of color. S.T.O.P. has significant experience advocating for New Yorkers' civil rights in opposition to dangerous and ineffective digital technologies.

Fight for the Future is a queer women led digital rights organization dedicated to defending our most basic rights in the digital age, protecting and expanding the Internet's transformative power in the lives of people. Fight battles against the unprecedented threats to Internet freedom, online privacy, human liberty, and free expression by resisting censorship, advocating for free speech and expression, demanding big tech accountability, and promoting antitrust legislation.

In its Request for Information, the Consumer Financial Protection Bureau (CFPB) (the Bureau) asked for accounts of data broker practices and impacts on the public. We respond to this request using our organizational expertise, rather than presenting a legal case for or against the Bureau's regulatory authority. We write jointly to relay our experiences with the data broker industry, urge the Consumer Financial Protection Bureau to consider the full range of the industry's impacts, and to support clarifying regulations that address harms such as discrimination, privacy violations, and data breaches caused by the unregulated collection, sharing, and retention of user data by the industry.

II. The Data Trade and its Ensuing Harms

a. The data broker industry and its practices

Data brokers are businesses that specialize in collecting and trading users' personal data. The Bureau should think of data brokers as entities that employs one or more of the following practices:

- Buying or selling data points in exchange for currency;
- Buying or selling access to data in exchange for currency;

Nearly every entity on the internet engages in these practices, some to a greater degree than others but crucially, the CFPB should consider distinctions in the nature of the entity and the scope of the data they trade when it develops regulations. For examples, the CFPB should consult state privacy laws, including the California Consumer Privacy Act (CCPA)[1] and New York's proposed Digital Fairness Act.[2] Both bills, and others,[3] recognize that states should regulate for-profit entities differently than universities, non-profits, and research institutions because they utilize data in different ways and pose different risks.

Data brokers collect and trade a range of identifiable user information. This includes but is not limited to how consumers use applications; detailed location histories; demographic information,

[1] Cal. Civ. Code § 1798.100.
[2] Digital Fairness Act, S. 2277, 2023-2024 New York Senate, Reg. Sess. (2023), https://www.nysenate.gov/legislation/bills/2023/S2277.
[3] *See eg.*, Virg. Code § 59.1-576.

including membership in legally protected groups, interests, affinities, and associations; and information about finances, property, healthcare, and wealth.[4]

Brokers source information in at least three ways, often in combination: (1) They collect data from a consumer's interactions online.[5] This could include, for example, an online or credit card purchase on a social media marketplace, interacting with a social media site, or submitting information in an online form. (2) Brokers may also collect information by licensing it from another broker.[6] For instance, CoreLogic licenses data from InfoGroup (now Data Axel).[7] (3) Some brokers scrape public sources for information and aggregate it into their proprietary products.[8] Two examples of entities collecting information in this way are CoreLogic, which amasses real property information from property records,[9] and Clearview AI, which scrapes social media sites and other sources to compile its database of facial images.[10] Brokers offer their products to a variety of customers, who use that information for a variety of purposes. Equifax, for example, a credit reporting agency, maintains and trades detailed credit histories, employment, and salary data which it has collected from a variety of sources.[11] They offer this information to lenders, credit card and insurance companies, and other businesses for marketing purposes.[12] Thomson Reuters, which claims it is not a credit reporting agency, offers comprehensive "cradle-to-grave" dossiers on individuals through its online platform CLEAR, including names, photographs, criminal history, relatives, associates, financial information, and employment information.[13] The company offers its products to both private and public clients.[14]

Once companies have collected user data, there aren't substantial regulations regarding how that data can and cannot be used. As a result, data brokers have free rein with user data which creates significant privacy and security concerns for users, their families and their communities.

b. <u>The industry's impact on consumers</u>

The industry's practices have a significant impact on consumers and the general public whose data is being scraped and traded. The process by which they amass data points from many sources and build consumer profiles which are packaged and sold to more companies or individuals gives consumers little to no choice in how their data is being collected, stored, and shared. Consumers

---

[4] "How Data Brokers Find and Sell Your Personal Info," *Norton Blog* (blog), January 18, 2021, https://us.norton.com/blog/privacy/how-data-brokers-find-and-sell-your-personal-info. "Meta Privacy Policy - How Meta Collects and Uses User Data," accessed June 6, 2023, https://www.facebook.com/privacy/policy/?section_id=1-WhatInformationDoWe. "Data Brokers," *EPIC - Electronic Privacy Information Center* (blog), accessed June 6, 2023, https://epic.org/issues/consumer-privacy/data-brokers/. https://techcrunch.com/2020/07/09/data-brokers-tracking/?guccounter=1. "Privacy Policy," CoreLogic, accessed June 6, 2023, https://www.corelogic.com/privacy-policy/.

[5] *See*, for example, Meta Privacy Policy.

[6] *See*, for example, Meta Privacy Policy. "Privacy Statement," Thompson Reuters, accessed June 6, 2023, https://www.thomsonreuters.com/en/privacy-statement.html.

[7] "Data Source," CoreLogic, accessed June 6, 2023, https://www.corelogic.com/wp-content/uploads/sites/4/downloadable-docs/capital-markets-data-sources.pdf.

[8] *See*, for example, Meta Privacy Policy. "Privacy Statement," Thompson Reuters.

[9] Privacy Policy, Corelogic.

[10] "Privacy Policy," Clearview AI, accessed June 6, 2023, https://www.clearview.ai/privacy-policy.

[11] "EXCLUSIVE: Your Employer May Share Your Salary, and Equifax Might Sell That Data," NBC News, January 30, 2013, http://www.nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066.

[12] "Data-Driven Marketing," Equifax, accessed June 6, 2023, https://www.equifax.com/business/marketing/.

[13] *Brooks v. Thompson Reuters*, 21-cv-01418-EMC (N.D. Cal. Aug. 16, 2021) (Amended Complaint).

[14] *Brooks v. Thompson Reuters*, (Amended Complaint).

cannot reasonably prevent brokers from collecting their data for many reasons. First, individuals are usually unaware that their data has been collected because data is collected by capturing information from online transactions, licensing between companies, and scraping public-facing websites. Consumers have no clear way to know when their data is collected, packaged, or traded.[15] The industry does not offer consumers meaningful notice or choice about whether to allow collection and sharing of their information. While some consumers may choose voluntarily to share their information for convenience, they are usually not offered the option affirmatively to opt-in or opt-out.[16] [17] When notice is provided, it is often collected through manipulative methods, like cookie banners that tell users to accept tracking or risk losing access to a website.[18] The mechanisms sites provide for consumers who wish to opt out are often hard to find, unwieldy, and even misleading. At the bottom of a Thomson Reuters' web page about CLEAR—only visible after scrolling past two or more pages of text—there is a link in small font that says: "For CA: Do not sell my information."[19] Beyond its presence in tiny font at the very bottom of this webpage, Thomson Reuters provides no notice to consumers of their right to opt-out.[20] Nor does the company enable California consumers to make use of the link easily. This robs consumers of their ability to make informed choices about their finances and purchases.

Although some companies voluntarily limit their collection and use of data to build public goodwill or to simplify their cybersecurity, ESG, or international compliance programs, companies' ability to collect and use data is generally unregulated in most U.S. industries.[21] Where the U.S. does regulate data, those regulations typically concern the *use* of data rather than the *collection* of it.[22] This means brokers can still collect any information they wish, even if there are some restrictions on using that data. Some U.S. laws give consumers the right to opt-out of data use in some circumstances, but this right is difficult to exercise.[23] The sheer number of companies that each consumer interacts with daily makes sending opt-out requests and following up on those requests impossible for most people.[24] Moreover, due to the lack of clear notice, consumers are generally not aware of which

---

[15] Eileen Brown, "Most Businesses Are Tracking Customers yet Don't Tell Them," ZDNET, December 16, 2020, https://www.zdnet.com/article/most-businesses-are-tracking-customers-yet-dont-tell-them/.
[16] "What If Opting out of Data Collection Were Easy?," Carnegie Mellon,naccessed June 6, 2023, https://www.cylab.cmu.edu/news/2021/01/12-opt-out-easy.html.
[17] William Stallings, "Online Privacy: Threats and Requirements," InformIT, 2020, https://www.informit.com/articles/article.aspx?p=2995362&seqNum=6.
[18] "We Need to Fix GDPR's Biggest Failure: Broken Cookie Notices" WIRED UK, accessed June 6, 2023, https://www.wired.co.uk/article/gdpr-cookie-consent-eprivacy.
[19] *Brooks v. Thompson Reuters,* (Amended Complaint). "CLEAR Investigation Software," accessed June 6, 2023, https://legal.thomsonreuters.com/en/products/clear-investigation-software.
[20] *Brooks v. Thompson Reuters,* (Amended Complaint).
[21] Phillip Walters, "CCPA: The Benefits of Voluntary Compliance," accessed June 6, 2023, https://www.truevault.com/blog/ccpa-the-benefits-of-voluntary-compliance. "The Benefits of Voluntary Compliance," accessed June 6, 2023, https://www.accountablehq.com/post/the-benefits-of-voluntary-compliance.
[22] Fredric D. Bellamy and Fredric D. Bellamy, "U.S. Data Privacy Laws to Enter New Era in 2023," *Reuters*, January 12, 2023, sec. Legal Industry, https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/.
[23] Consumer Reports, Comment Letter on Third Set of Proposed Regulations Implementing the California Consumer Privacy Act (Oct 28, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf.
[24] Aaron Sankin, "I Tried to Use the Ad Tech Industry's Tool to Opt Out of Personalized Ads. Did It Work? – The Markup," March 25, 2021, https://themarkup.org/privacy/2021/03/25/i-tried-to-use-the-ad-tech-industrys-tool-to-opt-out-of-personalized-ads-did-it-work . "Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?," Centre for Information Policy Leadership, accessed June 6, 2023, http://www.informationpolicycentre.com/2/post/2019/12/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses.html.

companies hold their data.[25] So, even consumers that have substantially enough free time to exercise opt-out rights cannot identify and contact every company that could have their information.

This mass collection, exploitation, and mismanagement of individuals' sensitive personal data by companies adversely impacts people of color, women, members of the LGBTQ+ community, religious minorities, people with disabilities, immigrants, economically disadvantaged people, and other marginalized groups. In many instances, the danger imposed upon marginalized communities by these companies replicates and amplifies existing inequities in society, reflecting historical biases that stem from unrepresentative or incomplete data, as well as flawed information.[26] Demographic factors also further inhibit consumers' ability to exercise control over their data, making privacy available only to the privileged. These factors include:

- Being Black, Indigenous, or a Person of Color. Police are more likely to surveil non-white people and include their information in biased data-driven policing systems.[27] Police frequently contract with data brokers for services that collect additional information about members of these already overpoliced groups.[28] This heightens risks to these communities by increasing demand for their information, making it harder to avoid data collection and use, and exposing them to more drastic harms, including a greater risk of incarceration.

- Being a lower income earner: People with lower income cannot afford privacy protecting services like automated or human agents that opt-out of data use on consumers' behalf, virtual private network subscriptions, or more expensive hardware that is not subsidized with ongoing ad revenue.[29] Likewise, those who work more than one job or take care of children have less time to read confusing data collection notices and exercise opt-out rights.

The impacts of these data practices are alarming. It is clear that they are engineered only to increase profits for the companies and so, the best interests or rights of users are not given meaningful consideration.

---

[25] "Too Little of Businesses?," Centre for Information Policy Leadership.
[26] Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/#footnote-6. Examining the intersection of data privacy and civil rights https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/
[27] "Garbage In, Gospel Out," NACDL - National Association of Criminal Defense Lawyers, accessed June 6, 2023, https://www.nacdl.org/Document/GarbageInGospelOutDataDrivenPolicingTechnologies.
[28] Press Release, "Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation," Electronic Frontier Foundation, September 1, 2022, https://www.eff.org/press/releases/data-broker-helps-police-see-everywhere-youve-been-click-mouse-eff-investigation.
[29] *See*, for example, some products, including Kindle offer ad supported versions that serve ads based on ad targeting. "2022 Black Kindle with 6'' High Resolution Display," Amazon, accessed June 6, 2023, https://www.amazon.com/dp/B09SWW583J?ref=erdcatpage_meetfam_i. "Amazon.Com Privacy Notice," Amazon, accessed June 6, 2023, https://www.amazon.com/gp/help/customer/display.html%3FnodeId%3DGX7NJQ4ZB8MHFRNJ.

c. Risks for Consumers

Data brokers are willing to sell information to anyone willing to pay.[30] This is not true for all brokers, as recognized Credit Reporting Agencies must comply with the Fair Credit Reporting Act, and other sector-specific privacy laws may restrain the collection, use, or sale of other types of information.[31] Other brokers choose only to sell services to law enforcement, private investigators, or fraud detection departments.[32] Even so, harms arise regardless of the purchasing entity's identity. In addition to exposing consumers to price discrimination and other economic harms, the trade in data entails risk to data subjects' rights of speech and association, facilitates predictive policing, and, on its own, constitutes a substantial violation of privacy.

i. Financial harms

Retail companies use data to favor some consumers over others, targeting them for price variations.[33] Data may show that people in a given geographic area are generally willing to pay higher prices than those in another.[34] An e-commerce company might therefore increase the price for a given product when IP addresses associated with that region view the product online. Data may also show that a high-net worth individual is a more valuable customer and select them for significant introductory offers that are not available to lower-income buyers who are less likely to be repeat purchasers.[35] Income is often correlated with race, and therefore income-based price discrimination can be racially discriminatory.[36] A 2020 study found that ride hail companies' data-driven pricing strategies led to higher prices in Black neighborhoods.[37]

Similarly, financial institutions use data to vary interest rates, giving some consumers less favorable loan and credit terms than others.[38] Several years ago, Meta patented a tool that analyzed a user's

---

[30] "How Data Brokers Steal & Sell Your Identity and How You Can Stop It," CyberGhost Privacy Hub, March 26, 2021, https://www.cyberghostvpn.com/en_US/privacyhub/data-brokers-put-a-price-tag-on-your-privacy-and-then-sell-it/. McAfee, "How Data Brokers Sell Your Identity," *McAfee Blog* (blog), August 2, 2022, https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/. "Data Brokers: Everything You Need to Know," Data Brokers: Everything You Need to Know, accessed June 6, 2023, https://www.avast.com/c-data-brokers.

[31] *See e.g.*, 45 C.F.R §§ 160.101-552, 164.102-106, 164.500-534 (HIPAA Privacy Rule); 16 C.F.R § 313 (GLB privacy rule).

[32] "Public Records Privacy Statement," Thompson Reuter, accessed June 6, 2023, https://legal.thomsonreuters.com/en/legal-notices/privacy-records.

[33] "Big Data Might Lead to Higher Prices," *Bloomberg.Com*, March 9, 2018, https://www.bloomberg.com/opinion/articles/2018-03-09/big-data-might-tell-retailers-which-consumers-to-charge-more. Etye Steinberg, "Big Data and Personalized Pricing," *Business Ethics Quarterly* 30, no. 1 (January 2020): 97–117, https://doi.org/10.1017/beq.2019.19.

[34] Manuela Battaglini, "How Users' Location Data Is Used for Price Discrimination," Transparent Internet, April 26, 2020, https://www.transparentinternet.com/data-ethics/how-user-location-data-is-used-for-price-discrimination/.

[35] "Returning Customers Are Worth 10x More than a New One," February 14, 2023, https://omnishopapp.com/blog/returning-customers-are-worth-10x-more/.

[36] "Big Data and First-Degree Price Discrimination," Bruegel, June 27, 2023, https://www.bruegel.org/blog-post/big-data-and-first-degree-price-discrimination. "Examining the Black-White Wealth Gap," *Brookings* (blog), February 27, 2020, https://www.brookings.edu/blog/up-front/2020/02/27/examining-the-black-white-wealth-gap/. "Bias Isn't the Only Problem with Credit Scores—and No, AI Can't Help," MIT Technology Review, accessed June 6, 2023, https://www.technologyreview.com/2021/06/17/1026519/racial-bias-noisy-data-credit-scores-mortgage-loans-fairness-machine-learning/.

[37] "Researchers Find Racial Discrimination in 'Dynamic Pricing' Algorithms Used by Uber, Lyft, and Others," *VentureBeat*, June 12, 2020, https://venturebeat.com/ai/researchers-find-racial-discrimination-in-dynamic-pricing-algorithms-used-by-uber-lyft-and-others/.

[38] "How to Talk About Big Data and Lending Discrimination," American Banker, September 10, 2015.

network of connections to determine creditworthiness.[39] The tool allowed a lender to examine the credit scores of a loan applicant's "friends" and factor that information into a credit determination. It is unclear if this product was ever offered to or used by lenders, but its discriminatory potential is obvious. Under this regime, an individual's creditworthiness would be evaluated at least partly on the basis of that person's social associations. Due to historical discrimination, de facto segregation, and the biased data driving these processes, Black borrowers, for example, are more likely to be associated with networks of lower net-worth and less history with the financial industry than white borrowers.[40] Holding this against Black borrowers would therefore translate directly to discriminatory lending practices.

Data driven banking can also make it harder for consumers to open new accounts. This is particularly true for people without a consistent address and/or identification documents, who are often among the most marginalized Americans. It is common for the financial services industry to use information purchased from data brokers for identity verification purposes, but doing so is unreliable.[41] If the consumer changes their address or job frequently, there will be mismatches in the information that they provide to the financial institution and the information that the financial institution buys from a broker.[42] When these mismatches occur, the financial institution often claims it cannot verify the individual's identity and blocks them from opening an account.[43] Compounding the problem, as the Bureau knows, consumers who experience housing or job instability are more likely to be underbanked and non-white.[44]

The data trade also can affect job prospects. Consumer reporting for employment is regulated by the Fair Credit Reporting Act, but formal reports are not the only searches that affect employment. As an example, some data brokers buy ads on websites to advertise their criminal history search services. An ad may say, "Three court records found for Jane Doe. Run a criminal record search." Even though Doe does not have a criminal background, this advertisement suggests that she does, which could affect her job prospects.[45] Further, if the name searched for were "Tamica Smith" rather than "Jane Doe," these ads would be significantly more likely to appear. A 2013 research study found

---

[39] Big Data and Lending Discrimination, American Banker. "Facebook Patents Technology to Help Lenders Discriminate against Borrowers Based on Social Connections," *VentureBeat*, August 4, 2015, https://venturebeat.com/business/facebook-patents-technology-to-help-lenders-discriminate-against-borrowers-based-on-social-connections/.

[40] "Separate and Unequal: Persistent Residential Segregation Is Sustaining Racial and Economic Injustice in the U.S," *Brookings* (blog), December 16, 2020, https://www.brookings.edu/essay/trend-1-separate-and-unequal-neighborhoods-are-sustaining-racial-and-economic-injustice-in-the-us/. "Bias Isn't the Only Problem," MIT Technology Review.

[41] "Identity Verification: The Complete Guide for Risk and Compliance," Unit21, accessed June 6, 2023, https://www.unit21.ai/blog/identity-verification-guide-for-risk-and-compliance. "Identity Verification API - Verify Users' Identities," Plaid, accessed June 6, 2023, https://plaid.com/products/identity/. "The Data Brokers Quietly Buying and Selling Your Personal Information," Fast Company, March 2, 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[42] "How Do Banks Verify Identity?," Youverify, accessed June 6, 2023, https://youverify.co/blog/how-do-banks-verify-identity.

[43] "How Do Banks Verify?," Youverify.

[44] "2021 FDIC National Survey of Unbanked and Underbanked Households," accessed June 6, 2023, https://www.fdic.gov/analysis/household-survey/index.html.

[45] "People Leaving Prison Have a Hard Time Getting Jobs. The Pandemic Has Made Things Worse," PBS NewsHour, March 31, 2021, https://www.pbs.org/newshour/economy/people-leaving-prison-have-a-hard-time-getting-jobs-the-pandemic-has-made-things-worse.

that Black sounding names were twenty five percent more likely to appear in advertisements for criminal records search services.[46]

ii. Speech and association

Data brokers chill speech and association. Many people are more reluctant to participate in protests, attend gatherings, or visit sensitive locations because of the risk of being tracked and identifiable.[47] Studies show that internet users are less willing to engage in political speech after being told that an internet service provider will monitor their activity.[48] This chilling effect causes damage to core democratic principles, and inhibits political participation and the free exchange of ideas. It is not only private companies contributing to this speech chilling activity, but also the U.S. government, which raises constitutional concerns. The U.S. buys millions of dollars' worth of data, including location information related to hundreds of millions of mobile devices and over 90% of the world's internet traffic.[49] In one egregious incident, the Oregon Attorney General's office investigated its own department head after it used internet monitoring tools to see that he had used the hashtag "#BlackLivesMatter" on Twitter and shared a logo for the rap group Public Enemy.[50]

iii. Policing

While police regulation is not within the Bureau's mandate, the Bureau's efforts to regulate data brokers will have downstream effects that improve local and national policing and safeguard against abuse. Data brokers fuel police practices that circumvent the Fourth Amendment. Policing agencies buy individual data and access to databases to view detailed personal information about individuals before establishing any suspicion of criminal activity.[51] They often manipulate this data into unwieldy predictive policing programs that try and fail to predict who will commit crimes and where they will commit them.[52] Immigration enforcement agencies also use this data to track all Americans, regardless of immigration status, and deport those who are undocumented.[53]

---

[46] "Google Searches Expose Racial Bias, Says Study of Names," *BBC News*, February 4, 2013, sec. Technology, https://www.bbc.com/news/technology-21322183.

[47] Zak Doffman, "Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology," *Forbes*, accessed June 6, 2023, https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/.

[48] Elizabeth Stoycheff, "Mass Surveillance Chills Online Speech Even When People Have 'Nothing to Hide,'" *Slate*, May 3, 2016, https://slate.com/technology/2016/05/mass-surveillance-chills-online-speech-even-when-people-have-nothing-to-hide.html.

[49] "DHS Tracked Americans, Foreigners with Cellphone Data in, Outside U.S.," NBC News, July 18, 2022, https://www.nbcnews.com/politics/immigration/dhs-spent-millions-cellphone-data-track-americans-foreigners-us-says-a-rcna38684. "US Military Buys Internet Monitoring Tool That Covers 90% of Web Traffic," IAPP, accessed June 6, 2023, https://iapp.org/news/a/report-us-military-buys-internet-monitoring-tool-that-covers-90-of-web-traffic/.

[50] "Black Lives Matter Report: Tweet Quoting Public Enemy Prompted DOJ Investigation," OPB, accessed June 6, 2023, https://www.opb.org/news/article/black-lives-matter-report-tweet-quoting-public-enemy-prompted-doj-investigation/.

[51] "US Military Buys Internet Monitoring," IAPP.

[52] "Garbage In, Gospel Out," NACDL.

[53] Johana Bhuiyan, "Revealed: The Contentious Tool US Immigration Uses to Get Your Data from Tech Firms," *The Guardian*, May 25, 2023, sec. US news, https://www.theguardian.com/us-news/2023/may/25/us-immigration-surveillance-google-twitter-meta-personal-data. "ICE 'now Operates as a Domestic Surveillance Agency,' Think Tank Says," *Engadget*, accessed June 6, 2023, https://www.engadget.com/ice-surveillance-report-us-government-193206600.html.

The risks of data driven policing become greater as more and more states criminalize essential and lifesaving healthcare, including abortion, gender affirming care, and hormone therapy.[54] States like Idaho that prohibit traveling out of state for abortions can use location data to track where its residents travel and identify who traveled with them, potentially with an eye towards charging pregnant people's loved ones as criminal accomplices for helping them during a difficult time.[55] States may also use consumer profiles to identify and predict who is likely to use gender affirming care, as they have done in other areas of law enforcement.[56]

III. Recommendations

a. Clarify the Fair Credit Reporting Act

It is within the CFPB's statutory authority to clarify FCRA regulations,[57] and the CFPB should exercise this authority to treat brokers' erroneous readings of the Fair Credit Reporting Act. Many data brokers argue they are not "Consumer Reporting Agencies" nor are they selling "Consumer Reports," and are therefore not subject to FCRA regulations. Rather, brokers claim to trade "credit header" information, meaning basic information like names, addresses, phone numbers, and social security numbers.[58] However, most uses for so-called header data bear "on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living;" the exact information the FCRA protects.[59] The Bureau should begin clarifying the industry's misunderstanding by explaining that "credit header" data is within the existing scope of FRCA regulations.[60] This will by no means address the full range of data broker harms, and the CFPB should consider using additional powers to promulgate even stronger regulations after clarifying credit header questions.

b. Mandate data minimization and transparency around data sharing

The industry does not provide a meaningful way for users to provide informed consent. Most users do not know how their information is collected, when it is shared, how or where to request its deletion. As data accrues, companies leverage it for profit and it is often used to craft discriminatory predictions about individuals and groups, which result in biased practices and policies that negatively

---

[54] "Pregnancy Panopticon," S.T.O.P. - The Surveillance Technology Oversight Project, accessed June 6, 2023, https://www.stopspying.org/pregnancy-panopticon.

[55] "Idaho Becomes One of the Most Extreme Anti-Abortion States with Law Restricting Travel for Abortions," NBC News, April 6, 2023, https://www.nbcnews.com/health/womens-health/idaho-most-extreme-anti-abortion-state-law-restricts-travel-rcna78225.

[56] "Garbage In, Gospel Out," NACDL. Molly Hennessy-Fiske, "Texas Attorney General's Office Sought State Data on Transgender Texans," The Texas Tribune, December 14, 2022, https://www.texastribune.org/2022/12/14/ken-paxton-transgender-texas-data/.

[57] CFPB Advisory Opinions Policy, 85 Fed. Reg. 77987, 77987–88 (Dec. 3, 2020).

[58] Fed. Trade Comm'n, 40 Years of Experience with the Fair Credit Reporting Act (2011).

[59] "Fair Credit Reporting Act" (CFPB, 2012), https://files.consumerfinance.gov/f/documents/102012_cfpb_fair-credit-reporting-act-fcra_procedures.pdf.

[60] "Request for Broad Consumer Financial Market Correction, Beginning with an Advisory Opinion Regarding Credit Header Data," February 8, 2023, https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/63e3ad622c78805f5de8125b/1675865443157/2023-02-08+Coalition+Letter+to+CFPB.pdf. Dell Cameron, "How the US Can Stop Data Brokers' Worst Practices—Right Now," *Wired*, accessed June 6, 2023, https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/.

impact marginalized and vulnerable communities. To address this, the CFPB should impose strict data minimization obligations on data brokers and ensure that individuals retain maximal control over their own personal data. Companies must also be required to proactively share how data is being used and transferred with both users and the general public.

c. Ensure data privacy and security of users personal information

After a private entity has collected consumer data, the onus must be on that company to ensure the security of said data. Frequent cyberattacks that expose peoples' personal, biometric, financial, and other data are a regular reminder of how the information companies collect is a target for hackers, data thieves, and other bad actors. In order to fully protect consumer data, the CFPB should require companies to regularly perform data privacy and civil rights impact audits. Such audits must be vigorous enough to ensure accountability for data security and transparency both around breaches and the company's own practices.

IV. Conclusion

Data brokers are buying, selling, and trading personal information without restriction, ignoring how they harm job prospects, banking, policing, and democratic freedom. These business practices won't end so long as there is money to be made, and the market is only increasingly rewarding data-first companies. The Bureau must move to regulate the worst of these harms, as there are minimal to no incentives for businesses to meaningfully change on their own. Please reach out to S.T.O.P. Legal Fellow and Program Associate, Evan Enzer, evan@stopspying.org, and Eseohe Ojo, Policy and Campaign Manager, Fight for the Future ese@fightforthefuture.org for any follow up.