Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

Comments
to the
Consumer Financial Protection Bureau
regarding
Docket No.: CFPB–2023–0020

by
Just Futures Law,
Mijente,
MediaJustice,
Surveillance Resistance Lab, and
UCLA Center on Race & Digital Justice

Filed on July 14, 2023

By notice published on March 21, 2023 the Consumer Finance Protection Bureau ("CFPB") requested comments from the public related to data brokers to assist the CFPB and policymakers in understanding the current state of business practices in exercising enforcement, supervision, regulatory, and other authorities.[1]

Pursuant to the CFPB's request, Just Futures Law, MediaJustice, Mijente, the Surveillance Resistance Lab, and the UCLA Center on Race and Digital Justice jointly submit this comment to call for urgent action to address and stop the immense harms of the data broker industry. In addition to our research, we share testimonies from five leading advocates across the country about their experiences with data brokers, and findings from a community survey we shared with our members and networks to solicit responses to the CFPB's individual inquiry questions. Our comment confirms the need for robust legal standards in the consumer information market that lawmakers noted in enacting the Fair Credit Reporting Act ("FCRA"),[2] and demonstrates how those concerns are more pressing with the exponential, unregulated growth of the data broker industry in the U.S.

We believe that not only does the business model of data brokers fall under the scope of the FCRA's definition of "consumer reporting agency,"[3] but that immediate action is needed to limit wide-ranging harms including human and civil rights violations. The FCRA should be updated to account to safeguard consumers' financial data against exploitation by the modern data broker industry, and the CFPB should exercise its rulemaking authority to protect consumers from unfair and deceptive acts and practices related to the handling of consumer data by consumer reporting agencies, financial institutions, credit card companies, and the data brokers intertwined in these industries.[4]

The CFPB's interventions are urgently needed, particularly for data brokers and other data analytics companies that provide the backbone of government surveillance schemes that target consumers, disparately impacting immigrant communities and Black, Indigenous, and people of color. Specifically, we call on the CFPB to:

- Issue advisory opinion and policies immediately, and to not wait for a long regulatory process;
- Close the "credit header" data loophole that allows for the sale of people's addresses, dates of birth, social security numbers, and phone numbers;
- Ensure data broker companies are bound by the privacy protections of FCRA, and to bring enforcement actions when those FCRA provisions are violated; and
- Ensure privacy protections apply to all law enforcement agencies and processes, with no law enforcement exception.

This comment and our recommended CFPB interventions draw on our years of research and work with impacted communities, as well as direct input from community members and advocates across the country. We organized a virtual town hall on data brokers and the CFPB's RFI on May 30, 2023, featuring

[1] "Request for Information: Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information," 88 Fed. Reg. 16951 (Mar. 21, 2023), *available at* https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection.

[2] 155 Cong. Rec. 2410 (1969) ("noting FCRA's purpose was to establish certain Federal safeguards over the activities of CRAs in order to protect consumers against arbitrary, erroneous, and malicious credit information."

[3] 15 U.S.C. § 1681a(f).

[4] Congress granted rulemaking authority to CFBP in FCRA (*See*15 U.S.C. 1681s) and in Gramm-Leach-Bliley Act 12 U.S.C. 5481(12)(J) (specifying provisions of Gramm-Leach-Bliley Act that qualify as "enumerated consumer laws" over which Bureau has jurisdiction).

leading advocates testifying to the impact that data brokers had on their lives, communities, and work, and creating space for community members to ask questions. As a follow-up, we created a survey for our networks and community members on their understandings and experiences, corresponding to the CFPB's questions in the RFI. Advocate statements and survey responses are included in Section 3 and Section 4. Speaker testimony and community survey results overwhelmingly show a deep need for the CFPB to take strong regulatory action to stop the harms of data brokers.

Our comment is divided into the following sections:

Section 1: About Our Organizations

Just Futures Law is a transformational immigration lawyering organization that provides legal support for grassroots organizations engaged in making critical interventions in the United States' deportation and detention systems and policies. JFL staff maintain close relationships with organizations and activists who seek to understand the scope and range of government surveillance and criminalization. JFL staff have decades of experience in providing expert legal advice, written legal resources, and training for immigration attorneys and criminal defense attorneys on the immigration consequences of the criminal legal system. JFL has a significant interest in the administration of government surveillance and data collection.

MediaJustice boldly advances racial, economic, and gender justice in a digital age by fighting for just and participatory platforms for expression. We harness community power through the MediaJustice Network of more than 70 local organizations to claim our right to media and technology that keeps us all connected, represented and free. www.mediajustice.org.

Mijente is a Latinx/Chicanx political, digital, and grassroots organizing hub that seeks to strengthen and increase the participation of Latinx people in the broader movements for racial, economic, climate, and gender justice through grassroots organizing, policy advocacy, and electoral mobilization. Mijente anchors the #NoTechforICE campaign (www.notechforICE.com).

The **Surveillance Resistance Lab** is a think and act tank focused on state and corporate surveillance as one of the greatest threats to migrant justice, racial equity, economic justice, and democracy. We challenge the surveillance state and how it increases corporate power and state violence as not just a threat to privacy, but also as a threat to fundamental rights. To counter this threat, the Surveillance Resistance Lab engages in investigative research, campaign incubation, advocacy, and organizing. We are committed to movement building to fight for accountability and government divestment from technologies that expand systems of control and punishment (as well as suppress dissent and difference) in public spaces, schools, workplaces, and at and across borders. www.surveillanceresistancelab.org.

The **UCLA Center on Race and Digital Justice** engages with a variety of network touch points including policy makers, scholars, activists, tech workers, and storytellers. With this community, we foster critical, sustainable, and scalable change at the intersection of race and digital justice. The Center focuses on who holds power, how to redistribute power, and the ways in which data and technology reflect power structures. We stay grounded, not abstract – it is the real experiences of people that motivate us, and real people for whom we work with to make change.

Section 2: Overview of the Harms of Data Brokers

This section directly addresses key questions from the market-level inquiries posed by the CFPB in this RFI, drawing on our organizations' combined years of research and work with impacted communities.

Background: Why the CFPB Can and Should Aggressively Regulate the Data Broker Industry

The CFPB can regulate the data broker industry because it oversees the enforcement of the Fair Credit Reporting Act (FCRA). Enacted more than 50 years ago, the FCRA protects consumers by limiting the disclosure of their personal data. It regulates consumer reporting agencies, telling them when and to whom it may disclose consumers' personal data. This includes disclosures to other businesses and, importantly, to government agencies, including law enforcement.

Since the FCRA became law, the number and type of consumer reporting agencies have grown way beyond the traditional Big 3 credit agencies of Experian, Equifax, and TransUnion. Today, many more businesses aggregate consumers' information from a variety of sources; process it to enrich, cleanse, or analyze it; and license it to other entities. We call these businesses data brokers, and we believe they are consumer reporting agencies within the meaning of the FCRA.

The CFPB should regulate the data broker industry because in the digital age, data brokers are capturing, centralizing, and selling consumer data on an unprecedented scale, and causing untold harm to consumers in the process.

For example, data brokers are currently cashing in on the unregulated trade of a set of key data points we call credit header data. Credit headers[5] are generated by traditional credit agencies, and they contain the key data points of name, birth date, Social Security number, residential addresses, and telephone number. This sensitive personal information of hundreds of millions of consumers in the United States currently receives no protection under the FCRA due to a mistaken interpretation of the law more than two years ago by the agency previously tasked with enforcing it, the Federal Trade Commission (FTC).[6]

The unregulated trade in credit header data facilitates data brokers' aggregation of data about particular consumers from a wide variety of data sources by enabling them to triangulate between the credit header data points and untold other sources. For example, a Big 3 credit agency like Experian may provide this data to another data broker and so on, until it flows together to one of the two major data brokers that aggregate data from thousands of sources, RELX and Thomson Reuters. These companies then sell access to hundreds of millions of comprehensive dossiers – which may contain errors about consumers – to public and private entities that may use them to deny a consumer access to housing, employment, or even to subject them to criminalization and deportation.

We urge the CFPB to address these severe consumer harms by immediately issuing policy guidance clarifying that the FCRA's protections against the disclosure of consumer report data apply to credit header data.

[5] "Credit header" was defined by the Federal Trade Commission in a 1997 report to Congress. *See* "Individual Reference Services - A Report to Congress" (Dec. 1997), *available at* https://www.ftc.gov/reports/individual-reference-services-report-congress.

[6] Fed. Trade Comm'n, 40 Years of Experience with the Fair Credit Reporting Act (2011) at 19–23.

Data Broker Data Collection, Data Sources, and Customers

This section addresses questions 1, 2, and 12 of the CFPB RFI's market-level inquiries.

1. *What types of data do data brokers collect, aggregate, sell, resell, license, derive marketable insights from, or otherwise share?*
2. *What sources do data brokers rely on to collect information? What collection methods do data brokers use to source information?*
4. *What specific entities and types of entities have relationships (e.g., partnerships, vendor relationships, investor relationships, joint ventures, retail arrangements, data share agreements, third-party pixel usage) with data brokers? Describe the nature of those relationships and any relevant financial arrangements pursuant to such relationships*
5. *Which specific entities and types of entities collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties?*
12. *Which specific entities and types of entities purchase data from data brokers? How do these entities use the purchased data?*

When community members seek essential services–such as water, internet, or phone service–or seek to meet basic needs such as housing or employment, they share highly sensitive personal data as part of the process with the entities administering those services. Unfortunately, this data is often collected and sold by data brokers with harmful results. In addition to the harms we expand upon below, these impacts can include:

- The sale of data to law enforcement agencies—who purchase large amounts of data to circumvent Fourth Amendment's warrant requirements—that disproportionately harms overpoliced communities.
- The sale of data about low-income communities of color to entities that will use that information to market predatory products, such as high-interest payday loans.

People should not have to fear that the information that they provide for basic necessities will be used to target them for criminalization, deportation, and predatory behavior. Unfortunately, this is the current practice because data brokers such as LexisNexis, which is owned by RELX, collect and sell personal data to thousands of customers, including U.S. Immigration and Customs Enforcement (see more below in Data Broker Impacts and Harms to Consumers).

Many data broker companies then sell consumers' financial data to public and private institutions that make very consequential decisions about people's lives.[7] For instance, child welfare agencies replace human decisions with data products that decide when a child is at risk of abuse or neglect. The Social Security Administration uses data brokers' data products to determine whether people getting government assistance had unreported assets that could disqualify them. Private lenders, landlords, insurance companies, banks, and employers also use data products to decide who to lend to, who to hire, and who might be a fraud risk. These data products purport to make short work of decisions and to make the work more efficient, but they cause errors and significant harms to people.[8]

Most worrisome, law enforcement agencies are major users of these products. Private companies, including data brokers that collect and sell products that include credit header data, are the backbone of

[7] Lamdan, Data Cartels pp. 41-42.
[8] Alice Holbrook and Nerdwallet, "When LexisNexis Makes a Mistake, You Pay For It," *Newsweek* (Sept. 26, 2019), *available at* https://www.newsweek.com/2019/10/04/lexisnexis-mistake-data-insurance-costs-1460831.html.

these surveillance systems. For years we have investigated how the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), other federal agencies, and state and local law enforcement agencies build massive digital surveillance systems through contracts with commercial entities, including those that collect and monetize consumer data.

For example, LexisNexis has long promoted its consumer data products as essential to counterterrorism and policing. After 9/11, LexisNexis provided tools that enabled racial profiling of Arab and Muslim men,[9] including Khalid Al-Draibi, a Saudi man who was falsely accused of involvement in the 9/11 attacks and deported from the United States.[10] In later publicity pitches for its "risk management" databases, LexisNexis emphasized its role in the Al-Draibi case, disregarding the false accusation at its core.[11] LexisNexis also funded multiple studies after 9/11 that called for vastly increased data collection and sharing.[12] In the 2000s, LexisNexis grew its counterterrorism and policing products, investing in companies that enable invasive data collection, analysis, and mass data sharing—many of which were known for privacy and civil liberties concerns. These companies expanded its ability to extract and repackage consumer data for police, DHS, and fusion centers:

- In 2004, LexisNexis acquired **Seisint**, the company behind the information sharing system **MATRIX**, which was pitched as a counterterrorism product and was used to expand Islamophobic policing power through mass data collection and surveillance.[13] MATRIX "scored" people based on their supposed terrorism risk, drawing interest from the federal government, and setting the stage for future data broker products that label people as threats.[14]
- Seisint had built **Accurint**,[15] which today is one of LexisNexis's key data sharing and analytics products, used by DHS and ICE.[16]

---

[9] César Muñoz Acebes, "Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees," Human Rights Watch (August 2002): 16 n.27, *available at* https://www.academia.edu/es/12299530/Presumption_of_Guilt_Human_Rights_Abuses_of_Post_September_11_Detainees_A_Human_Rights_Watch_report_%2016.

[10] Associated Press, "Saudi Cleared of Sept. 11 Role, but Gets 4 Months for Visa Fraud," *The New York Times* (Jan. 5, 2002, *available at* https://www.nytimes.com/2002/01/05/national/saudi-cleared-of-sept-11-role-but-gets-4-months-for-visa-fraud.html; William Matthews, "In the System," FCW, Jan. 20, 2002, https://fcw.com/workforce/2002/01/in-the-system/200746.

[11] Matthews, "In the System."

[12] Gary Gordon & Norman Wilcox, "Identity Fraud: A Critical National and Global Threat," Economic Crime Institute (2003), *available at* http://www.lexisnexis.com/presscenter/hottopics/ECIReportFINAL.pdf.

[13] "MATRIX: Myths and Reality," ACLU, last accessed Oct. 24, 2022, https://www.aclu.org/other/matrix-myths-and-reality; Robert O'Harrow Jr., "Anti-Terror Database Got Show At White House," Wash. Post, May 21, 2004, https://www.washingtonpost.com/archive/politics/2004/05/21/anti-terror-database-got-show-at-white-house/9499a352-aad1-4157-917b-c8e03221ad66. Robert O'Harrow Jr., "LexisNexis To Buy Seisint For $775 Million," Wash. Post, July 15, 2004, https://www.washingtonpost.com/archive/business/2004/07/15/lexisnexis-to-buy-seisint-for-775-million/6c876089-ddb9-4d30-a8d4-4aacb742de67.

[14] William J. Krouse, "The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project," CRS Report for Congress (Aug. 18, 2004) at 6, *available at* https://irp.fas.org/crs/RL32536.pdf; Associated Press, "Database Tagged 120,000 As Possible Terrorist Suspects," *The New York Times* (May 21, 2004), *available at* https://www.nytimes.com/2004/05/21/us/database-tagged-120000-as-possible-terrorist-suspects.html.

[15] News Release, "Seisint Launches Accurint: Breakthrough Technology Product To Speed The Search For Missing Children And Locate Criminals," (June 25, 2001), *available at* https://www.accurint.com/news/z_hold/news_6_25_2001.html.

[16] Sam Biddle, "ICE Searched LexisNexis Database Over 1 Million Times In Just Seven Months," *The Intercept* (June 9, 2022), *available at* https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/.

- In 2008, LexisNexis's parent company bought risk management company **ChoicePoint**, which became integral to fusion centers as well as police information sharing.[17]
- RELX's venture capital wing invested in **Palantir**, a data mining company that sells predictive policing software to police and fusion centers.[18] Mijente and other organizations have highlighted Palantir's role in ICE's deportation machine.[19]

Government agencies have been using data brokers and data analytics companies to bypass constitutional protections including the Fourth Amendment's warrant requirements, and procedural safeguards including the Privacy Act's systems of records notice and participation provisions.[20] Data broker and analytics companies help federal, state, and local governments actively "buy their way around" the constitutional provisions and privacy laws that protect consumers from invasive surveillance.[21] Immigration enforcement agencies, especially, rely heavily on private data companies to avoid complying with privacy requirements. DHS has called data brokers "mission critical" to their surveillance schemes.[22] This is, in no small part, because ICE agents dismiss the U.S. Constitution's warrant requirement and other procedural safeguards that protect consumers' rights as pesky, onerous obligations that, according to one account, "take too long."[23]

This use of mass surveillance tools like license plate readers, predictive policing analytics systems, biometrics collection, and other types of consumer data collection and analysis exposes more and more people to mass policing systems. Thus, the need for checks on these dragnet systems grows more urgent as the use of commercial surveillance technologies by government agencies proliferate.

Data Broker Impacts and Harms on Consumers

This section addresses questions 7, 13, and 16 of the CFPB RFI's market-level inquiries:

7. *How do companies collect consumer data to create, build, or refine proprietary algorithms?*
13. *What data broker practices cause harm to people? What are those harms and types of harms?*
16. *How can and does the activity of data brokers and their clients impact consumers beyond those whose data were collected or used by that data broker?*

Using data broker companies to bypass constitutional requirements is both an abuse of our rights and an activity that harms consumers. The data companies that participate in government tech surveillance programs are enabling the government to violate consumers' privacy, civil rights, and civil liberties.

---

[17] News Release, "LexisNexis Transformation Accelerates with Integration of ChoicePoint," LexisNexis (Oct. 15, 2008), https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-transformation-accelerates-with-integration-of-choicepoint.

[18] Joseph Menn, "Activist investors to pressure privately held Palantir on human rights," *Reuters* (Nov. 22, 2019), *available at* https://www.reuters.com/article/us-palantir-investors-idUKKBN1XW1XH; "TechFlash Q&A: Palantir investor thinks it could stay private forever (Oct. 18, 2016), *available at* https://www.bizjournals.com/sanjose/news/2016/10/18/techflashpalantir-investor-thinks-it-could-stay.html

[19] "Palantir Played Key Role In Arresting Families for Deportation, Document Shows," Mijente (May 2, 2019), https://mijente.net/2019/05/palantir-arresting-families.

[20] The Privacy Act of 1974, Pub. L. 93-57, codified at 5 U.S.C. 552a.

[21] Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment*?, WIRED (Feb. 11, 2020), *available at* https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/.

[22] *See* Funk, *supra* at note 9.

[23] Alfred Ng, "Privacy Bill Triggers Lobbying Surge By Data Brokers," *Politico* (Aug. 28, 2022), *available at* https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.

Because of the scale and scope of the data collected by data brokers, these violations are happening at an unprecedented degree. Tech surveillance is far more invasive than human intelligence-based surveillance and other types of information gathering not powered by tech companies. Data companies including LexisNexis provide ICE (and other government agencies that have the power to incriminate, arrest, and deport people) with billions of records from 5 billion devices and 2 billion digital identities, adding "hundreds of millions" of new records every day.[24] The government is giving these private companies tens of millions of dollars to superpower surveillance with products that provide "shopping malls for information," replacing warranted searches, in-person interviews, and other human-lead searches and seizures with a digital dragnet that sifts all of our data through it, catching everyone in a web of government surveillance.[25]

Not only do the companies sell consumers' data, they also sell predictions and prescriptions based on that data. The companies build analytics products designed to tell agencies who might commit a crime, who might associate with someone else, who might be at a certain place at a certain time. Products built by companies like Palantir,[26] PredPol,[27] and CopLink[28] push our personal data through algorithms and other data-churning systems, creating mosaics of our lives by piecing together billions of data points about us to "form an ever-evolving, 360-degree view" of our lives, revealing where we go, who we know, and what we do each day.[29] The policing agencies that contract with these companies can use their products to create visual webs of our associates and where we are located, and use that data to supercharge their surveillance programs.

It is difficult to identify the full extent of how these surveillant and predictive data technologies harm consumers because, due to lack of regulatory oversight and transparency requirements, these systems are largely invisible. In spite of the opaqueness of these products and services, researchers and investigative journalists have been able to identify some specific schemes that exemplify the industry, including:

- **LexisNexis provides a massive personal information platform to ICE**, fueling its ability to track, target, detain, and deport people.[30] LexisNexis states that its consumer databases include 10,000 different data points on hundreds of millions of people, with its product often marketed to law enforcement. Previously, **ICE bought up access to utility data on more than 170 million people** from the National Consumer Telecom & Utilities Exchange, via **data broker Thomson Reuters** and **credit bureau Equifax**.[31] Most people who provide their information for cable, phone, and electricity bills have no idea their data–including addresses and Social Security

[24] Sam Biddle, "LexisNexis to provide giant database of personal information to ICE," *The Intercept* (Apr. 2, 2021), *available at* https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/.
[25] Just Futures Law and Mijente, "The Data Broker to Deportation Pipeline: How Thomson Reuters & LexisNexis Share Utility & Commercial Data with ICE," *available at* https://www.flipsnack.com/justfutures/commercial-and-utility-data-report/full-view.html.
[26] *Gotham*, PALANTIR, https://www.palantir.com/platforms/gotham/.
[27] PREDPOL, https://www.predpol.com/.
[28] *Advanced Crime Analytics Platform*, COPLINK, https://forensiclogic.com/coplink/.
[29] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L. J. 628, 628–79 (2005); Funk, *supra* at note 9.
[30] Biddle, *supra* at 15 and 16.
[31] Drew Harwell, "Utility giants agree to no longer allow sensitive records to be shared with ICE," *The Washington Post* (Dec. 8, 2021), *available at* https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

numbers—would be shared this way.[32] The NCTUE has since agreed to end the sale of utility data, but regulation is needed to restrict use of existing data and future data sharing.

- **Location data from Muslim prayer applications, collected by data broke X-Mode without consumers' knowledge,[33]** has been resold and used by U.S. military contractors and other government entities even without the company's permission. This example shows that data brokers themselves are not able to follow their promises of consumer privacy, and face no consequences when the invasive information they gather is abused and resold after its collection. X-Mode, like other data brokers, boasts about the location data it gathers on over 50 million people, including from other sensitive sources like family safety and LGBTQ dating apps.
- **Marketing company Mobilewalla used secretly collected mobile location data to track protesters after the murder of George Floyd**, characterizing participants by race, gender, and religion.[34] Mobilewalla states that it buys up location data via aggregators, covering 80-90% of phones in the US. Similarly, despite claims they would not engage in domestic surveillance, the **controversial AI company Dataminr helped police monitor nonviolent protests after the murder of George Floyd**, including sharing locations.[35]

People's Rights, Consent, and Control over Their Own Data

This section addresses questions 9, 10, 11, and 15 of the CFPB RFI's market-level inquiries.

9. *Can people avoid having their data collected?*
10. *Under what circumstances is deidentified, "anonymized," or aggregated data reidentified or disaggregated?*
11. *Can people reasonably avoid adverse consequences resulting from data collection across different contexts (e.g., cross-device tracking, re-identification, mobile fingerprint matching)?*
15. *What actions can people take to gain knowledge or control over data, or correct data that is collected, aggregated, sold, resold, licensed, or otherwise shared about them?*

Consumers usually do not know that their data is part of these companies' products, nor do they agree to have their data bought and sold by the entities that build the nation's surveillance systems. Even when people are aware, they cannot often avoid having their data collected, especially when that is a prerequisite to accessing essential services and resources, such as utility hookups and housing. In effect, consumers can take virtually no meaningful actions to wholly take control of their data or prevent its collection, use, misuse, and selling by data brokers and other parties, as default data collection and opt-in systems are the default across most of the country. Opt-out systems also are not a solution in themselves,

---

[32] *See supra* at note 23.
[33] Jon Keegan and Alfred Ng, "Lawsuit Highlights How Little Control Brokers Have Over Location Data," *The Markup* (Mar. 21, 2022), *available at* https://themarkup.org/privacy/2022/03/21/lawsuit-highlights-how-little-control-brokers-have-over-location-data.
[34] Caroline Haskins, "Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location," *BuzzFeed News* (June 25, 2020), *available at* https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying; Zak Doffman, "Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology," *Forbes* (June 26, 2020), *available at* https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6f7c143d4a1e.
[35] Sam Biddle, "Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr," *The Intercept* (July 9, 2020), *available at* https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

as they put the burden on the individual consumer and are rarely transparent or easy to access or understand.

As an example, LexisNexis' opt-out system[36] demonstrates the severe limits—and consequences—of opt-out options currently made available by data brokers. First, for a consumer to protect their personal information via opting out, the notice says they have to give LexisNexis sensitive information, which can include Social Security number and address. Second, the notice explains that opting out can limit people's ability to access online services such as car insurance and identity verification. Third, it states there is no way for people to remove their information or opt out of their information's inclusion in certain LexisNexis products shared with law enforcement, products regulated by FCRA, "third party data available through real time gateways," news, and legal documents.

The companies that participate in these government data surveillance markets profoundly impact consumers' lives, even when consumers do not consent to participate in data collection. "Consent" to share personal data is not full and true when it is the only way a consumer can access a resource that they desperately need, or when consumers cannot know or fathom the scope of the data collection and its uses. In the case of data brokers, consumers rarely know what data is collected, how the data collected on them may be used or sold, who it is being sold to, how it can be used for criminalization or decision-making about their lives, and the web of third party companies and public entities engaged in selling, repackaging, and sharing our data. Data brokers' current "consent" frameworks grossly fail to fulfill consumer rights-focused frameworks, such as Consentful Tech, which defines consent as freely given, reversible, informed, enthusiastic, and specific.[37]

Many data companies claim to protect consumers by anonymizing consumers' data, but anonymization is a myth. De-identified data can easily be re-identified when combined with other data points.[38] In fact, Thomson Reuters, a company that sells its data products to ICE and other government agencies, promises it can identify consumers who do not want to be identified by matching disparate pieces of data, making people go from "invisible to stark visibility."[39]

Data Broker "Controls," Safeguarding, and Accuracy

This section addresses question 18, 19, and 21 of the CFPB RFI's market-level inquiries.

18. *What controls do data brokers implement in order to protect people's data and safeguard the privacy and security of the public? Are these controls adequate?*
19. *What controls do data brokers implement to ensure the quality and accuracy of data they have collected?*
21. *Are there companies or other entities that help consumers understand and manage their relationship to, and rights with respect to, data brokers? If not, why not? What factors could further help such consumer-assisting companies and entities?*

[36] https://optout.lexisnexis.com/.
[37] https://www.consentfultech.io/.
[38] Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TechCrunch (Jul. 24, 2019).
[39] *What Investigators Can Learn From People Who Want to Disappear*, Thomson Reuters (Dec. 3, 2019), https://legal.thomsonreuters.com/blog/what-investigators-can-learn-from-people-who-want-to-disappear/.

The very design and nature of the data broker industry is predatory in at least two ways. First, it engages in mass collection and sharing of data to law enforcement agencies, causing documented harms to protected classes of people. Second, it sells data to companies for targeted advertising to shape consumers' behavior. In this environment, any supposed safeguards or controls instituted by data brokers to ensure privacy, security, quality, and accuracy of their data are insufficient, due to the inherent power imbalances that the industry perpetuates.

To date, government agencies have taken too much of a hands off approach to ensuring that data brokers adhere to strict safeguards around data protection, retention, accuracy, and security. Government entities purchasing data broker products and information often do not ensure the accuracy of this data. As an example, the Department of Homeland Security's Office of Biometric Identity Management recommends—but does not require—that data providers for the Homeland Advanced Recognition Technology System (HART) follow certain best practices and guidelines around data and places the onus on "the original data owner" to be "responsible for ensuring the accuracy, completeness, and quality of the data submitted to OBIM."[40] This can apply to both government and private entities such as data brokers. Based on extensive research, our organizations have raised urgent concerns that HART will vastly expand DHS' surveillance capabilities and supercharge the deportation system, collecting and sharing invasive data on over 270 million people including juveniles.[41]

Efforts to help consumers understand and manage their relationship to, and rights with respect to, data brokers are similarly insufficient, due to the power imbalance of the industry. Placing the onus on individual consumers, who lack both information about the scope of data brokers' information on them and power to impact its use, cannot address the collective harms of the industry on consumers, especially protected classes of people.

CFPB Supervision, Enforcement, and Rulemaking

This section addresses question 22 of the CFPB RFI's market-level inquiries.

22. *How might the CFPB use its supervision, enforcement, research, rulemaking, or consumer complaint function with respect to data brokers and related harms?*

The CFPB must regulate the whole industry to protect consumers from companies engaged in government data and surveillance markets. Regulating only specific types of data brokers will be insufficient to fulfill CFPB's mandate of protecting consumers. Until now, data companies have largely been given a pass to operate in secrecy when they work with government agencies on law enforcement and surveillance initiatives. But in order to fully protect consumers, the entities that sell data and data analytics systems to government agencies should be subject to consumer protection rules even when their products are being used for law enforcement and other national security purposes.

These are the types of activities that not only should be addressed by Congress and limited by courts, they are also violations of consumer protection guarantees that CFPB has the power to regulate. The agency

[40] US Department of Homeland Security (DHS), "Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA), DHS/OBIM/PIA-004," (Feb. 24, 2020), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf, p. 22.
[41] Immigrant Defense Project, Just Futures Law, and Mijente, "HART Attack: How DHS' massive biometrics surveillance will supercharge surveillance and threaten rights," *available at* https://surveillanceresistancelab.org/wp-content/uploads/2023/01/HART-Attack-2022.pdf.

should explicitly subject all data brokers to their scrutiny, including the firms that sell government surveillance products. Firms like Palantir and RELX should not get a pass to gather, sell, and otherwise exploit consumers' data behind a veil of secrecy just because they are working with law enforcement and national security agencies. The government should also not get a pass to build dragnet surveillance systems through these third-party corporations.

See specific recommendations for regulatory action in Section 5.

Section 3: Advocate Testimonies

Our five organizations organized a virtual town hall on data brokers and CFPB's RFI on May 30, 2023, featuring speakers testifying to the impact that data brokers had on their lives, communities, and work. Their written testimonies and short bios are included here with their consent.

A. Statement of Claudia Marchán
Executive Director of Northern Illinois Justice for Our Neighbors
Plaintiff in lawsuit against data broker LexisNexis

Bio: Claudia Marchán was born in Monterrey, Nuevo Leon in Mexico and immigrated to the US at the age of 4. Claudia grew up in Chicago and brings her own experience as a DACAmented immigrant to her work. Claudia serves as Executive Director of Northern Illinois Justice for Our Neighbors, bringing a background in community organizing, community development and financial management. Through NIJFON, Claudia is also active in the Illinois Coalition for Immigrant and Refugee Rights, and Claudia's local community work also includes Quality-of-Life Planning in Chicago neighborhoods.

Until fairly recently, I had no idea what data brokers were, exactly, or how their collection and sale of personal data impacted me, my family, and my community in Harwood Heights and Chicago. That all changed about a year ago when I discovered that my personal information was in an online database called Accurint, which is owned by the private company LexisNexis. I was curious to know what information this company had about me, and I was worried that it could be used against me or against those close to me, so I requested a copy.

I was shocked when I got the 46-page packet of information about me and people around me. 46 pages. It had my Social Security Number – all the numbers written out, none redacted – all the different addresses where I have lived at throughout my life – I don't think they missed a single address – emails, phone numbers, you name it.

How did this company gain access to so much information about me? I realized through working with Mijente that basic things like opening an account with a phone company or connecting to utilities could lead to LexisNexis having my personal data.

And then, they turn around and sell it not just to other private companies, but to law enforcement, to agencies like ICE, agencies with the power to arrest and deport. They do this around state laws like the Trust Act that prohibit sharing of information to agencies like ICE.

When I first found out about this, I felt anxiety, and it was keeping me up at night. At that point I had just become a legal permanent resident of this country, and before that I had DACA. But not everyone in my family has those protections. My worry and my fear was for them.

I thought, how is it possible that police and ICE can get access to all this personal information without having to get a warrant or even tell a court about what they're doing? I never even knew this was happening, so how could I have possibly given consent for all of this surveillance?

It was very upsetting to think that after all our immigrant communities have fought for, winning local policies that made our city a sanctuary jurisdiction, how can ICE go shamelessly around those protections with a click of a button on a computer, and put a target on our backs?

All this made me want to take action to inform and protect my family and my community. In my role as Executive Director of Northern Illinois Justice For Our Neighbors, I get questions from immigrant community members and clients who are nervous about providing data to companies, even when they need it to access utilities or build their credit. I remember I was once there. I want folks in that situation to be able to trust that when they seek essential services, that information is not going to be used against them by ICE and police. They should feel safe to be able to go about their daily lives and get the things that they need to live without worrying about who can track their information.

This is the future I am fighting for – for my kids, my family, and my community. It is important that members of our community take note of what is happening and know that we have a voice and that we can take action to stop these harmful practices that can lead to family separations. Everyone has a voice and through community action and advocacy we can make our voices heard and ensure that companies stop these harmful practices. It is long past time that federal regulators take on data brokers and do more to prevent harms like the sale of our data to ICE. I am glad you are here today, learning about these issues, and that we are taking action, together, to create a future without fear that seeking electric or phone service could lead to ICE at our doorstep.

B. Statement of Carl Hamad-Lipscombe
Executive Director, Envision Freedom Fund

Bio: Carl Hamad-Lipscombe is Executive Director of Envision Freedom Fund and a veteran movement builder, organizer and campaign strategist. Envision Freedom Fund works to dismantle the unjust and oppressive criminal and immigrant legal systems while meeting the critical needs of individuals impacted by those systems in the present.

The Impact of Data Brokers on Undocumented Immigrants
I deeply appreciate the opportunity to share the concerns of the community of formerly detained immigrants that I work with here in New York. As Executive Director of Envision Freedom Fund, one of the largest immigration bond funds in the country and the only such organization in the New York / New Jersey / Connecticut Tri state area, I have learned firsthand of the effects that data brokers can have on the lives of immigrant community members, particularly undocumented and Black immigrants.

As you are aware data brokers collect, analyze, and sell vast amounts of personal information, usually without an individual's knowledge or permission. They collect data from a wide range of sources, including no public records, social media platforms, and commercial databases, and compile comprehensive profiles that are used for targeted advertising, background checks, credit scoring, and host other purposes. While data brokers can affect anyone's privacy and security, their impact on undocumented immigrants is particularly severe.

Data Brokers Make Undocumented Immigrants Vulnerable to Exploitation
First, undocumented immigrants often lack access to financial services and are forced to rely on alternative methods for meeting their basic needs. Data brokers exploit this vulnerability by selling information to unscrupulous actors who prey on immigrants.

For example, employers may use this information to identify and exploit undocumented workers by paying them below minimum wage, stealing their wages or subjecting them to unsafe working conditions.

Landlords may exploit their housing needs by charging exorbitant rents or engaging in unfair eviction practices. Scammers may use personal information to deceive immigrants into paying for fraudulent services or to threaten them with deportation if they do not comply.

In our communities we call some of these fraudsters "notarios." They claim to be able to help immigrants remain in the US by filing immigration applications. And then after the individual or their family has paid thousands of dollars, they disappear. I'm particularly worried right now as asylum seekers are welcomed to our cities, that data brokers are increasing the likelihood that they will encounter nefarious actors who will target them for exploitation.

Data Brokers Perpetuate a Climate of Fear
Second, undocumented immigrants already live in constant fear of being identified and deported.

By aggregating and selling personal data, including addresses, phone numbers, and social connections, data brokers make it easier for immigration enforcement agencies and malicious actors to locate individuals. This increased visibility can result in heightened surveillance, arrests, detentions, and family separations. The loss of privacy perpetuates the climate of fear and undermines the trust between immigrant communities and government agencies, making it more challenging for undocumented immigrants to access basic services, report violence, or seek help when needed.

Data Brokers Increase the Risk of Criminalization
In addition, data brokers often rely on algorithms that have outdated or incorrect information to create profiles. Immigrants - both undocumented and documented (e.g. green card holders) who may have complex circumstances, are at a higher risk of being misidentified or having their information inaccurately represented. This can result in targeting, discrimination, and stigmatization, making it even more difficult for individuals to access social services, employment, or housing opportunities. For example - and I've heard of so many cases of this within Black immigrant communities - an incorrect criminal record attributed to an individual may lead to their wrongful arrest or denial of employment opportunities. I also worry about the likelihood of individuals ending up on lists of blacklisted tenants, no fly lists, or gang and "terrorist" databases maintained by law enforcement.

Undocumented Immigrants Have Little Recourse
Lastly, undocumented immigrants in particular face significant barriers when trying to seek recourse for the harm caused by data brokers. Due to their precarious legal status, some may be hesitant to come forward and report abuses or pursue legal action for fear of drawing attention to their immigration status. And, the lack of specific legal protections for undocumented immigrants creates further obstacles in holding these companies accountable for their actions.

I'm going to refrain from offering specific policy recommendations because this isn't my area of expertise, but I will say this - our communities need agencies like the CFPB to use every tool at their disposal to protect us from these companies.

C. Maru Mora Villalpando
Organizer, Co-Founder of La Resistencia and Latino Advocacy

Bio: Maru Mora Villalpando is a community organizer and immigrant. She was born and raised in Mexico City In the U.S., she has spent more than two decades working for racial justice and immigrant rights. She is the founder of La Resistencia, the group's main focus is to end all detentions and

deportations, and to shut down the Northwest Detention Center in Tacoma, Washington. Maru is also a founding member of Mijente, a national digital organizing Latinx group. Due to her work against Immigration and Customs Enforcement, the agency put her in deportation proceedings in 2017. Despite these challenges, Maru, her family and her community remained undeterred and continued their community work. In September 2021 Maru was granted prosecutorial discretion by the same agency that tried to deport her, and with this recent win Maru continues the work to end all detentions and deportations in Washington State where she currently lives.

My experience [with data brokers] was one that literally changed my life. We've been fighting ICE and their terror campaign against immigrants for many years. I had no idea in December of 2017, when somebody knocked on my door, that it was the mail person with a letter from ICE to me. It was a Notice to Appear, which meant that the deportation proceedings against me just began. There was absolutely no reason for them to start this process, except that I do the work I do. And it was because of litigation that ICE admitted that my anti-ICE work and Latino Advocacy work were the reasons, besides being undocumented, for me to be in the deportation proceedings.

The surprising thing, though, is how did they get my address? My address was private. I didn't share it with anyone, precisely because I wasn't documented, precisely because I knew who I was fighting. Through litigation, we found that the CLEAR database [run by Thomson Reuters] had sold all my information to ICE. I got, I don't know how many pages in my CLEAR report. I didn't count them because I was just reading and reading and reading: All the home addresses where I have lived. Everything about my marital status, divorce status, my child. Everything that they could find. They used over 30 combinations of my name to see what they could find. There was absolutely nothing that they could use against me, except the fact that I do this work.

This thoroughly changed my life because my work has been focused on fighting ICE and immigration detention and shutting down the private detention center here in Tacoma – and all of the sudden I had to switch to survive this deportation proceeding. It was very clear that they did this because they wanted us to stop. ICE uses these companies to come after organizers like me. They use this information to create a chilling effect, when we learn that they can just grab anything about our lives. I had no idea that buying insurance for my car would lead to all this data being shared with them.

We fought so hard in our state to also have sanctuary laws to prevent ICE from coming in and getting information from our Department of Licensing. And they just go around it. We work with people and we learn again and again that they have no contact with ICE, they were hiding because they were undocumented, yet ICE got their information. Again, we have really strict laws in our state that prevent that from happening. But ICE is a huge, very well-funded organization and is using our taxpayer money, my taxpayer money, and our undocumented taxpayers money to buy this information and come after us.

These companies [selling data to ICE] need to be stopped. There are things that can be done right now as basic as not allowing them to sell our names, our date of birth or our addresses, like it happened to me. ICE sent me that Notice to Appear because the data brokers knew where I lived –and nobody else knew, except them. It is very clear that ICE will do anything under its power to come after us. Data brokers, first of all, they shouldn’t exist, because my data shouldn't be for sale in the first place. But they also should not be involved in the deportation machine. They should be stopped and there are ways that that can happen right now without having to wait for a really long rule making process.

D. Statement of Tracy Rosenberg
Executive Director, Media Alliance

Bio: Tracy Rosenberg has worked as Media Alliance's Executive Director since 2007. She has organized and advocated for a free, accountable and accessible media system, blogs on media policy and is published frequently around the country. Tracy sits on the board of the Alliance for Community Media Western Region, serves on the anchor committee of the MediaJustice coalition and co-coordinates Oakland Privacy, the Bay Area, California surveillance coalition that works regionally to defend the right to privacy and enhance public transparency and oversight. Oakland Privacy won a Pioneer Award in 2019 and a James Madison Freedom of Information Award from the Society of Professional Journalists in 2021.

My name is Tracy Rosenberg and I am the Advocacy Director for Oakland Privacy, a citizens group that advocates for privacy regulations with respect for civil rights and community consent and the director of Media Alliance, a Northern California democratic communications advocate. In these dual roles, I have come to recognize the powerful role data brokers play in the surveillance economy and the ineffectiveness of most existing privacy regulations in addressing the data broker market.

My state, California, has without a doubt been one of the most aggressive states in pursuing state-level privacy-protective legislation. The CCPA, followed by the CPRA ballot initiative, and joining Vermont as the only other state to establish a data broker registry, which now lists over 500 data brokers. This year, California is considering a bill SB 362 to have our department of justice establish a global opt-out for people to ask for their information to be deleted from data brokers en masse.

Yet even with all of this, as advocates, it feels like we are chasing the proverbial nine-headed hydra. Whatever we do, the problems continue due to the massive size and scale of the industry and the impunity with which it operates. Data brokers run the gamut from huge and proto-respectable giants like Thomson Reuters and Axicom to the sketchiest fly by night "peoplefinder" websites. Companies with virtually blank websites turn out to be location data vendors who sell our travel patterns to the highest bidder through grabbers embedded in seemingly innocuous alarm clock, calendar, wallpaper or dating apps.

Sources for data broker information run the gamut from publicly available records not often aggregated to caches of data held by technology companies and financial institutions, but what is often not highlighted is the circulation of information between data broker networks. One of the biggest sources of data broker information is … other data brokers. Between the Vermont and California registries excluding duplicates, there are over 800 different companies. This points to the literal impossibility of keeping one's information out of their hands. Even if you track down one or two third party entities and go through some sort of delete or accuracy check process, the information has probably already circulated to hundreds of others entities within the larger data broker universe. Like gossip, PII spreads like wildfire.

Data brokers absolutely traffic in sensitive information about protected characteristics. Race, age and gender pronouns are basics in almost any data broker profile. The myth of "tech objectivity" is laughable when the systems are built to suck in human characteristics and to infer any that are missing. As far back as a 2013 Senate report, it was noted that one of the biggest advertising industry brokers was selling profile datasets with titles like "Rural Households Barely Making It" and "Ethnic Second City Strugglers" for targeted marketing – likely to predatory loan companies. In a nutshell, what this data broker economy is based on is using our personal information to label us according to some of our deepest vulnerabilities so it can deliver the most vulnerable to those that make money from exploiting us.

This works in several ways: Peoplefinder websites, which number in the hundreds if not thousands and often have everchanging and similar names in an effort to outwit the companies affluent Americans pay to get themselves out of them, enable doxxing, harassment, abuse and domestic violence. Predatory finance companies target people in financial distress with balloon loans and refinancings that can lead to economic ruin down the line. Law enforcement circumvents warrant requirements by acquiring bulk geolocation data that can supercharge racial profiling without meeting any probable cause or even reasonable suspicion requirement.

The negative downstream impacts of the third party data economy impacts everyone, but it hits harder on Black and Latinx people, poor people, seniors and people with limited English fluency. Lack of income prevents using services to prevent some information from getting to data brokers, by using paid VPNs or phone apps that cost money, for example or for using the services that remove PII from some third party sites. Lack of a 24/7 robust Internet connection and lack of digital savvy prevents using opt out and removal requests and and lack of time makes the whack-a-mole game even harder to play. Data profiles, especially those that are incomplete or inaccurate, perpetuate redlining and financial discrimination and aggregate biased criminal justice data linked to overpolicing with limited credit histories to limit opportunities. Unregulated health app data can expose mental health issues including dementia and memory loss to predatory scams, both legal and illegal. In short, the data broker economy works to ensure that any personal vulnerability can and will be used against us in exchange for the convenience technology provides, which is often a really bad bargain.

Self-regulation has been a failure. There are too many data brokers, and while the biggest companies may have some incentive to limit their customer base, the hundreds and possibly thousands of shady quick-appearing ones have no such incentive. They just want to sell to whoever buys. Those that serve law enforcement use the excuse of "security" to operate in the shadows and once one is exposed, new ones rush in to fill the gap.

Here is the first page of CA Data Broker Registry: PrivCo Media LLC, Convex Labs, Inc., Alliant Cooperative Data Solutions, LLC, SheerID, Inc., Structure, FourthWall Media, Inc., Affinity Answers Corporation, Unearth Campaigns, LLC, PLEXUSS, INC., Meltwater News US Inc., Imprint Analytics LLC, MightyRep, Preferred Communications, Warmly Inc, Disco Technology Inc. AdAdapted Inc., Gale, Health is Wealth Marketing LLC DBA PickMedicare, Precisely Software/PlaceIQ, Equifax Data Services LLC, Saha Ventures LLC, iWave Information Systems Inc., PossibleNow Data Services, Inc., All Good Media LLC, Distribution Processing Center LLC.

With the exception of Equifax, do you even know of any of these companies? And yet they know all about you.

D. Statement of Mark Toney
Executive Director, The Utility Reform Network

Bio: As Executive Director of The Utility Reform Network since 2008, Mark aligns the TURN legal, organizing, legislative and communication staff to fight for affordable, sustainable and safe energy, broadband and phone service for all California residents, with a special focus on low-income households, communities of color, immigrants, and rural communities. Mark was appointed to the Board of Trustees of the California State Bar, and serves on the boards of ACLU Northern California, National Whistleblower

Center, and California Shakespeare Theatre. Mark served as executive director of Center for Third World Organizing for four years, and for Direct Action for Rights & Equality for eight years. He holds a B.A. from Brown University, a Sociology Ph.D. from UC Berkeley, and his leadership has been recognized as a Kellogg National Leadership Fellow, National Science Foundation Fellow, and Mother Jones Heroes for Hard Times.

I am Mark Toney. I'm an organizer by trade, a sociologist by discipline, and a troublemaker at heart. I've served for 16 years as Executive Director of TURN (The Utility Reform Network). TURN believes that we can and should live in a society where power, broadband, and phone services are treated as basic human rights for all.

has led the fight to win privacy protections for California smart meter customers. Collecting utility usage data every few minutes can reveal what appliances a customer uses when they're at home and when they leave and return on a daily basis. The smartphone privacy campaign mobilized grassroots communities and privacy advocates to keep utility usage data out of the hands of data brokers and immigration enforcement agencies. TURN, MediaJustice, the Privacy Rights Clearinghouse, and other allies won a 2011 ruling by the California Public Utilities Commission that prohibited utility companies and third party contractors from releasing smart meter usage data without the affirmative consent of each customer for each request. So the default in California is opt in, for each individual every single time, not a default opt out like it works with credit cards. Now the only exception is a court-ordered subpoena.

The American Civil Liberties Union published a report in 2017 that showed that from 2012 to 2016, San Diego Gas and Electric released smart meter data usage for over 13,000 customers – by far the highest number of any California utility, despite being one fourth the size of the other utilities. Further research revealed targeting of immigrants, as most of the data releases were to ICE and other federal immigration agencies, which were taking advantage of a loophole that gives those agencies the authority to issue their own subpoenas. So TURN led the campaign to enact legislation to require federal agencies to get a court order prior to them receiving smart meter data. Assembly Bill 2788, adopted in 2020, protects the privacy of utility customers, especially immigrant residents from harassment from federal law enforcement agencies.

We in California have done our part. We need the Consumer Financial Protection Bureau to do your part. We have done everything we can to prohibit utility companies from selling private customer smart meter usage data to data brokers and other third parties. We need the CFPB to step in and adopt rules now that prohibit utility companies from selling private customer address and contact data to data brokers and other third parties. You at the Consumer Financial Protection Bureau have the power to realize one of President Franklin D. Roosevelt four freedoms: Everybody, regardless of immigration status, deserves freedom from fear.

Section 4: Community Survey Responses to the CFPB's Individual Inquiry Questions

At our May 30, 2023 town hall, we shared a community survey to solicit responses from our networks, community members, and advocates across the country. The survey was open until June 6 and received 42 responses. We have selected key responses here that answer the CFPB's Individual Inquiry Questions, as well as address several Market-Level Questions. A full compilation of anonymized responses is included in Appendix A.

Overall Trends:
The survey responses reflected several trends that demonstrate the need for full and urgent action by the CFPB:

- Individuals cannot fully know what data brokers have collected on them, cannot know what specific information is shared, and cannot see or correct incorrect data. Only the CFPB has the authority to fully understand the practices of these secretive companies and take action.
- Individuals cannot protect their basic rights from abuse and violations by data brokers.
- Even impacted community members and advocates working in areas deeply affected by data brokers' are not fully aware of the harms of the industry. It is not possible for individuals to understand these secretive practices or to fully protect themselves.

Background Questions:

We started the survey with four questions to assess people's understanding of data brokers and awareness of what information is collected on them, as a background to the CFPB's Individual Inquiry questions.

Community Survey Question: How did you learn about data brokers?
While about half of the responses to this question seemed to define "what data brokers are" rather than explain how the respondent learned about data brokers (21 responses), a key theme that emerged in the responses was that people learned about data brokers from advocates and organizers familiar with data brokers, from people directly affected by data brokers, or from work in a previous job (12 responses). This makes it clear that people are not learning about data brokers through data brokers themselves, underscoring the opacity of the industry. Of the responses that specifically named who or how the respondent learned about data brokers, the majority of respondents learned about data brokers from people directly harmed by data brokers or were directly impacted by data brokers via their own work. A handful of quotes spoke to how the learning about data brokers happened after a harm or data breach had occurred. One respondent talks about this very issue:

> *"Colorado launched a drivers licenses for all program in 2014, which allowed undocumented immigrants to access state licenses and IDs. In 2019, we received reports from community members who believed their driver license application and information was shared with ICE, so we started to investigate. Our investigation revealed that information was not only being shared with ICE directly by state employees, but they were also able to access information through state and national databases and automated networks and that much of the data was being bought or sold and ending up in the hands of data brokers."*

As noted in the quote above, not only did this respondent learn about data brokers after directly affected community members informed them about fear of a potential harm, their investigation also discovered that the harm and breach of privacy had already been occurring. Responses like this also underscore that people are not learning about data brokers from the industry itself, nor are they learning about data brokers from the government. Despite law enforcement's heavy use of data from data brokers and despite current efforts from the CFPB, FTC, and other federal agencies to highlight data brokers in their comment request processes, our respondents were more likely to hear about data brokers from advocates and organizers than the government itself. Only one respondent said that they learned about data brokers from a government website.

Community Survey Question: Do you know what information data brokers have collected on you?

- Yes: 28
- No: 14

While a majority of respondents said they knew what information data brokers have collected on them, we believe this could reflect a lack of understanding of the general scope of data collected by data brokers—or reflect that our audience for the survey was largely impacted people and advocates who have learned about data brokers through their lives and work.

Community Survey Question: Can you tell when a specific data broker has sold your information and to whom?

- Yes: 8
- No: 34

Community Survey Question: Do you know what information is collected by data brokers on other people in your community/ies, and how this compares to your data?

- Yes: 10
- No: 24

CFPB Individual Inquiry Question 1: Have you experienced data broker harms, including financial harms? What are those harms?

Community Survey Question: How have data brokers impacted the lives of you and your community? For example, what harms or potential harms have you experienced from the selling of your personal data?
Of the 42 responses to the question, over 70% said that the harms they've experienced from data brokers related to data breaches, identity theft, and spam calls. The frequency with which these harms were mentioned in the responses shows that the harms of data breaches, identity theft, and spam calls are the most visible and therefore most forefront to our respondents. While it is easy to write off these harms as minor annoyances, especially when they are viewed in isolation of one person experiencing spam calls or spending individual time to address identity theft, the impacts of these harms are much deeper. When looked at in aggregate, data breaches, identity theft, and scams can drastically harm people's lives, work, finances, and personal security.

One respondent speaks to this in their experience of seeing enough individual cases to see how they add up when looked at in aggregate.

> *"In the first place, it's a violation to not know what's "out there" and available about you. Second, data breaches are something everyone's now subjected to--people's info (that they*

probably didn't fully realize had been amassed by various corporations/entities for profit) being compromised to hostile third, fourth, and fifth parties, making them vulnerable to identity theft, all manner of scams, and other assaults (even physical assaults & loss of liberty/life, not just assaults, thefts re: data/info). It can affect people's credit, damaging their ability to live their life in this world where credit can determine so many things. It can lead to mix-ups in name/identity that ruin a person's life. It can lead to "criminal justice" issues, including the aforementioned issue of mix-ups--the wrong people get swept up in all kinds of things & w/o their knowledge, & once (if) they learn about it, it's too late. People's health and disability statuses being revealed can cause still other issues. Plus, it's not necessarily "just" the person whose personal information is compromised; it can affect extended family & other close relations/known associates. There are so many ways they're harmful & have impacted folks I've come into contact with over the years--I could go on forever. I work in legal aid and I've seen some really horrible things in people's files, where through no fault of their own, they're in a mess they can't fix, and sometimes, even a lawyer with access to tons of tools and agencies and alleged "available remedies" can't fix."

As noted in the response above, not only is the harm across a community cumulative, but even for the individual, a seemingly small harm can develop into deeper and long-lasting or permanent harms. What seems like a small harm can spawn into harms like denial of access to opportunities or increased criminalization because of the linkages between our data bodies, others' data profiles, and how our data are used in various decision making processes. Often because there is no explanation in these decision making processes, people (individuals or communities) do not know that data from a data broker led to a harmful decision with deeper repercussions than a spam phone call. These negative deeper impacts are often worse for Black, Brown, and immigrant communities.

Respondents also talked about fear of harm to themselves, a community, or a family member, including impacts related to criminalization, surveillance, and barriers to accessing essential services (approximately 6 responses). A fear of potential harm is also a harm in itself. Fear of harm changes behaviors and pushes people into proactively denying themselves services or products that come with data visibility and can create a chilling effect for those who wish to speak out and exercise their First Amendment and other rights. Below are some examples of responses related to this feeling of fear:

"I continuously get phishing emails which I'm sure is due to the sale of my personal data. My father is susceptible to scams, and I fear that he will be put in financial danger as data brokers continue to sell all of our data."

"I worry about friends and acquaintances who may not have been born in the US, including many of the people I grew up with. I also worry about surveillance of people seeking abortion or even just birth control in parts of the country where it is now outlawed and queer people as anti-lgbtq sentiment is stoked across the country again. And frankly, I worry about people outside my immediate communities. We all deserve safety."

"Data brokers have made our undocumented community members feel unsafe and paranoid about accessing vital services. My organization has been trying to connect people with the Affordable Connectivity Program, a $30 discount on monthly internet plans, but we've had to tell people they were ineligible because we could not guarantee that ICE wasn't collecting their data. We want people to have access to internet, but we do not want to jeopardize their safety either."

Lastly, responses to this question brought up societal harms that the data broker industry has caused or could cause (approximately 5 responses). Responses discussed the impact of data brokers on deportations and breaking up of communities, instability in democracy and information manipulation, and the meaning of consent. While it might be easy to say that the data broker industry does not necessarily create these harms, the data broker industry allows, exacerbates, and accelerates these societal harms. As one respondent who formerly worked in the data broker industry says:

> *"As a former marketer, I have to say, I left the industry because of this ecosystem of companies and practices. I couldn't do the work in good conscience. I'm willing to bet a lot of marketers feel the same way but they aren't in a position to leave. The best marketers don't feel good about being predators, manipulating consumers on a minute-by-minute basis, but that's what data brokers and data analytics practices in the marketing industry allow brands and other marketers to do. They're not just manipulating an individual's consumption of goods and services, they're manipulating that individual's ability to discern truth from fiction in regards to the world around them, their social and professional relationships, their own identity, their own reputation, and their access to insurance, credit, work, safe housing and legal recourse. They're a vector for the dissolution of democracy itself."*

The industry cannot be left to regulate itself. Seeing this long list of individual, community-level, and societal harms, the only choice for the CFPB is swift, strong, and intentional intervention.

<u>Community Survey Question: Data brokers may collect and sell highly personal information about you. How does that make you feel?</u>

In response to this question, the overwhelming majority of responses indicated negative feelings. Respondents mentioned feeling unsafe (approximately 3 respondents), uncomfortable (approximately 3 responses), angry and annoyed (approximately 5 responses), worried and scared (approximately 8 responses), and 16 respondents said *"This is a crime, taking my personal information and privacy for profit."* One respondent expressed multiple of those sentiments:

> *"Exploited. Not in control of my life. When everything from location data, to datasets that affect credit score, to employment history....even though I've lived a clean life and have never broken the law, I'm treated like a criminal. I don't know what the data is, but I suspect there's wrong data being sold about me. It causes worse damage than gossip or slander because the data moves faster and... does anyone actually have the ability to remove inaccurate data from the system, including the dark web? No. It's a wicked problem."*

<u>Community Survey Question: Data brokers often sell people's highly personal information to law enforcement agencies. How might this impact you and your community?</u>

The majority of the responses to this question discussed bringing unnecessary danger and problems to communities. In particular, more than 1 out of 4 responses brought up the theme of criminalizing everyday behavior and how law enforcement agencies and other actors can use data to create stories that makes someone seem like a criminal. Here are some examples of those responses:

> ***"****I am Mexican and American Indian. There is almost no one in my life unlikely to be subjected to abuse by law enforcement on a daily basis, and their access to more info about us than what we*

*look like and where we live, that we're poor people of color in poor neighborhoods, only makes abuse *more* likely. It's terrifying."*

"Everyone is guilty of something, even if it's going 26 mph (or 24 mph) in a 25 mph zone. Having grown up next to a town where the cops pulled you over for both of those things, I'm aware that such petty offenses may be thrown out of court, but I worry that any such ticket issued in the past 10 years may be permanently logged by data brokers where it can be pulled up and used as a prior offense or evidence for a warrant now."

"My personal information was shared with law enforcement agencies, and I could be the subject of an investigation. Even if I have committed no crime, my personal information may be used to monitor, track or investigate me, which will affect my daily life and work."

"As a pregnant person, laws are being passed that criminalize our existence. With the overturning of Roe, highly personal information (buying a pregnancy test at CVS, searching pregnancy symptoms on Google, location data at a Planned Parenthood) may be weaponized for the criminalization of people with certain pregnancy outcomes."

Respondents continued to discuss how data brokers collecting their data and sharing it with law enforcement leads to feelings of distrust and takes away their privacy (8 responses).

CFPB Individual Inquiry Question 3: Are you able to detect whether harms or benefits are tied to a specific data broker? Are existing methods of detection adequate?

Community Survey Question: Can you tell when a specific data broker has harmed you?
- Yes: 15
- No: 27

CFPB Individual Inquiry Question 4. Have you ever attempted to remove your data from a specific data broker's repository for privacy purposes?

Community Survey Question: Have you tried to remove the data maintained by a data broker on you?
- Yes: 5
- No: 30

CFPB Individual Inquiry Question 5. Have you ever attempted to view or inspect the data maintained about you? If so, describe your experience.

Community Survey Question: Have you tried to view the data maintained by a data broker on you?
- Yes: 6
- No: 30

CFPB Individual Inquiry Question 6. Have you ever attempted to correct your data? If so, describe your experience.

Community Survey Question: Have you tried to correct the data maintained by a data broker on you?
- Yes: 4

- No: 30

CFPB Individual Inquiry Question 7. Have you taken any other steps to protect your privacy or security as a result of data broker harms? Were these steps adequate?

Community Survey Question: Have you taken any other steps to protect your privacy or security as a result of data broker harms?

- Yes: 17
- No: 18

Community Survey Question: Do you believe it is possible to protect your privacy and security from data brokers?

- Yes: 17
- No: 25

CFPB Market Level Inquiry Question 22. How might the CFPB use its supervision, enforcement, research, rulemaking, or consumer complaint functions with respect to data brokers and related harms?

Community Survey Question: Do you believe the government has taken adequate steps to protect your privacy from data brokers?

- Yes: 23
- No: 13

Community Survey Question: What do you think the CFPB should do to limit the surveillance power of data brokers?

A key theme in responses was limiting and regulating the industry's power and ability to collect our data. Half of the respondents specifically mentioned consent as a key framework of that regulation. The most nuanced answers about consent emphasized models of opt-in consent. For example, one respondent wrote:

> *"Automatically opt everyone out of this sort of surveillance. Let data brokers ASK to be let into our lives, and provide services worth the surveillance in exchange. Some people may find it worthwhile (e.g. when they choose the services of Smart Homes)."*

Many respondents brought in the economic logic of the industry into their recommendations, demanding that the CFPB not let data brokers sell information for profit and/or bring enforcement action in the form of penalties, fines, and fees for damages for data brokers who have harmed people – about 1 out of 3 responses. It is clear that even if a majority of respondents think that the government has taken steps to protect their privacy from data brokers, they still see that much more can be done with proper enforcement.

Section 5: Recommendations for CFPB Action

It is essential that the CFPB take immediate action to curb this rogue data broker industry. This section answers question 22 from the CFPB's market-level inquiries, on the CFPB's authority and regulatory action it can take.

While we fundamentally believe that the data broker industry is so harmful that it should not exist, the CFPB does have the authority and power to regulate the industry now and mitigate current harms. The CFPB oversees the enforcement of the Fair Credit Reporting Act (FCRA), the first federal law to regulate the use of personal information by private businesses. The FCRA limits the circumstances under which consumer reporting agencies (a broad term that should encompass data brokers) may disclose consumer's personal data. Data brokers are consumer reporting agencies in that they compile consumer reports. Especially considering the wide definition that the CFPB presented in its RFI on data brokers, we should remain aware that CFPB has the ability and authority to enforce FCRA on any company that is a part of the consumer reporting, data profile creation process.

Immediate actions that CFPB can take now include:

1. **Issue an advisory opinion and policies immediately, and do not wait for a long regulatory process.** CFPB has been silent on whether it will take any other agency action on data brokers, such as issuing policy guidance, which it could do right now. While we understand the importance of formal rules and regulations, these often take many months if not years to issue as they go through a lengthy notice and comment process (and often subject to litigation.) We urge the agency to act with urgency and issue policy guidance now, and not wait until the conclusion of a lengthy rules process to take action to protect consumers.

2. **Close the "credit header" data loophole that allows for the sale of people's personal information.** Currently, companies are allowed to sell people's personal information including address, DOB, SSN, and phone numbers (also known as credit header data) to third parties due to old agency guidance that says that such information is not protected under the FCRA. This means when someone hands over this data to apply for a service (e.g., utilities, housing) and the company runs a background check on the person, this sensitive information is sold to third parties. CFPB should stop this surveillance practice.

3. **Ensure data brokers are bound by the privacy protections of FCRA, and bring enforcement actions against data brokers that are failing to comply with FCRA.** Right now, many data brokers operate in a legal gray area and argue that they are not consumer reporting agencies and therefore do not need to comply with the FCRA. The CFPB must clarify, to the fullest extent possible, that data brokers are subject to the FCRA including its privacy restrictions. Data brokers are unequivocally part of the process of creating consumer reports and cannot continue to pass along liability to other actors in the ecosystem. Examples of enforcement action that the CFPB can bring against data brokers include requiring the data broker to delete all wrongfully obtained data, issuing monetary penalties, and disgorgement of proprietary algorithms created from consumer reports and data profiles. We expect and encourage the CFPB to use all enforcement tools at their disposal to protect consumer rights.

4. **Ensure the FCRA's privacy protections apply to all law enforcement and processes, with no law enforcement exception.** Lawmakers who enacted FCRA were clear that they intended it to restrict warrantless information sharing with enforcement, an intent that the CFPB must honor and effectuate. For example, when a consumer reporting agency collects consumer data to determine a person's eligibility for utility, housing, or employment, it cannot share this data with law enforcement unless there is a court order or grand jury subpoena. In clarifying how the FCRA applies to data brokers, CFPB must ensure that strong privacy protections apply not just to companies but also to law enforcement use.

These are just some of the immediate actions that the CFPB can and must take to protect consumers. If CFPB fails to act and waits until this long process of formal rulemaking happens, the CFPB will be complicit in the continued harms against consumers across our country.

Appendix A: Full Community Survey Responses
CFPB Request for Information on Data Brokers

Survey Background:
The Consumer Financial Protection Bureau (CFPB) issued an RFI for information on data brokers in March 2022, requesting information from community members to inform how it regulates the industry.

In response, MediaJustice, Mijente, Just Futures Law, the Surveillance Resistance Lab, and the UCLA Center on Race and Digital Justice created a survey based on the CFPB's question, to help our networks and members compile information and feedback on the impact of data brokers and what the CFPB should to do to curb the power of these surveillance corporations. Members of the public were able to contribute your testimony by filling out this survey, in May and June 2023.

Anonymity: Responses have been compiled and shared anonymously by the five organizations.

Response Overview:
We received 42 responses, in both English and Spanish. Responses were received from a diverse group of people, including members of immigration and racial justice organizations such as the Colorado Immigrant Rights Coalition, the Georgia Latino Alliance for Human Rights (GLAHR), Make the Road New York, Muslim Advocates, and Public Counsel.

Responses:

Required Questions

How did you learn about data brokers? (42 responses total)
Key theme: advocacy, civil society, past work

- I learned about data brokers through the American Dragnet, a 2022 report published by Georgetown Law's Center of Privacy and Technology. The report detailed how data brokers were selling data from ISPs, public utility companies, and DMV records to government agencies like ICE.
- Probably over a decade ago, now, b/c I was doing work w/ an organization placed under surveillance, and had to become familiar w/ surveillance techniques, encryption, and all sorts of data/info security issues.
- Community website
- Working on development of the Trust Policy for Fairfax County Virginia. The Trust Policy was designed to protect Fairfax's immigrant community by preventing the County from releasing personal information that might end up in the hands of ICE.
- an old job
- Through my work & the news
- I suppose I learned what data brokers were called and just how much harm they can cause through listening to people involved in immigration law and criminal justice, including immigrants (both documented and undocumented), lawyers, protestors, and more. I've also learned how to use social media marketing, which is definitely connected.
- I learned about data brokers in my past work, such as demanding Big Tech companies (like Google) to stop collecting data related to pregnancy status and outcomes after the overturning of Roe.
- Colorado launched a drivers licenses for all program in 2014, which allowed undocumented immigrants to access state licenses and IDs. In 2019, we received reports from community members who believed their driver license application and information was shared with ICE, so we started to investigate. Our investigation revealed that information was not only being shared with ICE directly by state employees, but they were also able to access information through state and national databases and automated networks and that much of the data was being bought or sold and ending up in the hands of data brokers.
- I learned about data brokers as a law student from the #NoTechForICE on campus and though events hosted by immigrants' rights organizations.
- Mijente y la campaña No Tech for ICE
- GLAHR

Additional responses:

- Personal data, consumer information and other privacy on the Internet. *[14 respondents had same response]*
- Personal information such as consumption record, movement track, online shopping address. *[5 respondents had the same response]*
- Oral transmission *[2 respondents had same response]*
- Website of the government
- Facebook
- LinkedIn
- Social media
- On social media
- Big data through the Internet
- It is public

- A Data Broker is a business that aggregates information from a variety of sources.
- It's diverse

How have data brokers impacted the lives of you and your community? For example, what harms or potential harms have you experienced from the selling of your personal data? (42 responses total)

Key theme: individual harms (ex: data breaches, identity theft, and spam calls)

- My personal information was leaked and I got a lot of phone calls from telemarketers trying to sell products. *[16 respondents had same response]*
- I used to get a lot of calls from people trying to sell products, and it really affected my life. *[3 respondents had same response]*
- I receive many calls from companies that I do not recognize nor have I solicited information from them .
- Data brokers have collected and sold my and my family's information to public and private actors without my consent. Nearly no person I know has understood the vast extent of information on them that is available for purchase. No one knows that some data brokers sell their license plate tracking information to private investigators. No one knows that they can be located with a single search by data brokers' consumers. People do not know this because no data broker has actually sought informed consent.
- I've had pieces of my identity stolen, requiring cancellation and reissuance of items. I understand that members of my communities have faced surveillance and discrimination due to data brokers' sale of personal data.
- A lot of fear.
- I continuously get phishing emails which I'm sure is due to the sale of my personal data. My father is susceptible to scams, and I fear that he will be put in financial danger as data brokers continue to sell all of our data.
- I get a lot of crank calls
- Sometimes there are unwanted cold calls.
- I get text messages all the time
- Because they can collect, store and analyze personal data and then use it for AD targeting, marketing and other purposes.
- Personal privacy disclosure: Data agents may sell your personal information, such as name, address, email, mobile phone number, etc., to third party advertising companies or other institutions, which may lead to your personal privacy disclosure and your personal information may be used improperly.
- Sometimes it reveals some privacy
- Fraud and identity theft: They may use this information to commit fraud or identity theft, such as opening credit cards, taking out loans or buying other goods and services by forging identities.
- Identity theft: Hackers may use a person's identity to create fake social media accounts or other online activities, which can cause significant financial and reputational damage.
- Privacy breach: The sale of personal data by data brokers may result in the disclosure of personal privacy, which poses a threat to the security of individuals and communities. Malicious third parties, such as hackers or criminals, may use the personal information to commit fraud, identity theft and other illegal acts.
- Word gets out, gets looked at differently

Key theme: communal and societal harms

- I worry about friends and acquaintances who may not have been born in the US, including many of the people I grew up with. I also worry about surveillance of people seeking abortion or even just birth control in parts of the country where it is now outlawed and queer people as anti-lgbtq

sentiment is stoked across the country again. And frankly, I worry about people outside my immediate communities. We all deserve safety.

- Data brokers have made our undocumented community members feel unsafe and paranoid about accessing vital services. My organization has been trying to connect people with the Affordable Connectivity Program, a $30 discount on monthly internet plans, but we've had to tell people they were ineligible because we could not guarantee that ICE wasn't collecting their data. We want people to have access to internet, but we do not want to jeopardize their safety either.
- We believe that data brokers are responsible for the increased surveillance and targeting immigrant communities in Colorado. In particular, we increasingly see immigrants followed and arrested by ICE through the use of license plate reading technology. We also see ICE relying on technology provided by data broker companies to track detainees in local jails and arrest individuals outside of jails or courthouses when they are released on bond or have completed their sentences.
- Deportation of undocumented immigrants is an ongoing problem in Fairfax County
- The sale of information to ICE
- In the first place, it's a violation to not know what's "out there" and available about you. Second, data breaches are something everyone's now subjected to--people's info (that they probably didn't fully realize had been amassed by various corporations/entities for profit) being compromised to hostile third, fourth, and fifth parties, making them vulnerable to identity theft, all manner of scams, and other assaults (even physical assaults & loss of liberty/life, not just assaults, thefts re: data/info). It can affect people's credit, damaging their ability to live their life in this world where credit can determine so many things. It can lead to mix-ups in name/identity that ruin a person's life. It can lead to "criminal justice" issues, including the aforementioned issue of mix-ups--the wrong people get swept up in all kinds of things & w/o their knowledge, & once (if) they learn about it, it's too late. People's health and disability statuses being revealed can cause still other issues. Plus, it's not necessarily "just" the person whose personal info is compromised; it can affect extended family & other close relations/known associates. There are so many ways they're harmful & have impacted folks I've come into contact with over the years--I could go on forever. I work in legal aid and I've seen some really horrible things in people's files, where through no fault of their own, they're in a mess they can't fix, and sometimes, even a lawyer with access to tons of tools and agencies and alleged "available remedies" can't fix. There are, of course, more general, everyday annoyances that come w/ data brokers: the junk mail, robo calls, political machinery harassing you via text & phone & email for your vote & your money. It's ALL bad, all-around.
- Look into B2B companies such as Acxiom, Oracle and similar companies who hold "anonymized" 360 degree online behavioral data about consumers. Their value proposition to their business clients is that they collect all kinds of online and offline data about individuals, in real time, and they know everything about us. They connect all the datasets about a single person into one profile. They have been collecting location data for many years, and this puts all people at risk. They claim it's anonymous, but let's be honest....if you know that much about a person you can infer their identity. These data brokers are the ones doing the real harm in the name of "marketing," supposedly. They use their "marketing" data to interfere with elections, by partnering with organizations like Cambridge Analytica and identifying populations to "suppress," then sending them messages on social media that deter them from showing up to election polls. This is what happened in the 2016 US Presidential election, and this is how Trump, to his total surprise, got elected President. The word "suppression" gets used by the most nefarious companies in the data ecosystem, including Intelius, which I write about below. I predict that voter suppression will be done by the social media platforms themselves in pending US elections. For example, Twitter is partially funded by Oracle, and this conflict of interest puts US (and other countries such as Turkey, etc.) elections at extreme risk. Since Elon Musk's takeover of Twitter, content on the platform has skewed to the far right. This is well-documented.

Mr. Musk has been discrediting the press, which is a tactic out of the authoritarian playbook, and if he succeeds in dissolving the credibility of the media and simultaneously developing Generative AI systems with OpenAI (he still maintains an informal business relationship with CEO Sam Altman), he can algorithmically flood Twitter with disinformation in the form of generative text and images. Without accountability through Section 230, platforms like Twitter can get away with permitting inaccurate and harmful information to proliferate, causing the fragmentation of the social fabric and acceptance of the norms of democracy. The risk is created through the confluence of several factors: Musk discrediting the media and promoting "citizen journalism" (which can also be disinformation from bots and far-right influencers), allowing generativeAI and algorithmic proliferation of disinformation powered by Oracle data, publicly shaming Jewish billionaire George Soros who funds Democrat candidates, providing Twitter Spaces speaking opportunities to far-right presidential candidates and conveniently declining to follow through with the equivalent gesture to Democrat candidates. I'm sure there are other tactics at play. As a former marketer, I have to say, I left the industry because of this ecosystem of companies and practices. I couldn't do the work in good conscience. I'm willing to bet a lot of marketers feel the same way but they aren't in a position to leave. The best marketers don't feel good about being predators, manipulating consumers on a minute-by-minute basis, but that's what data brokers and data analytics practices in the marketing industry allow brands and other marketers to do. They're not just manipulating an individual's consumption of goods and services, they're manipulating that individual's ability to discern truth from fiction in regards to the world around them, their social and professional relationships, their own identity, their own reputation, and their access to insurance, credit, work, safe housing and legal recourse. They're a vector for the dissolution of democracy itself. Take action RIGHT NOW, CFPB.

One no response

- no

Data brokers may collect and sell highly personal information about you. How does that make you feel? (42 responses)

Key theme and top response: taking my personal information for profit is a crime

- This is a crime, taking my personal information and privacy for profit. *[16 respondents had same response]*

Key theme: Worry, fear

- Very vulnerable and threatened by super-vigilance.
- It makes me feel extremely scared.
- feel nervous and scared
- I'm afraid I'm going to get involved in this.
- You may feel very insecure and confused.
- The collection makes me worried for my safety.
- Preocupado.
- Apprehensive

Key theme: Anger

- I was angry that these people would take advantage of my privacy and put me in danger. *[3 respondents had same response]*
- You may feel pain, anger and disappointment.
- I'm primarily just annoyed by all of the little inconveniences I go to in the name of trying to avoid giving data to those data brokers, but just because I'm lucky now

Key theme: Uncomfortable

- It can be very uncomfortable and uncomfortable.
- Extremely uncomfortable. My information is not a commodity.
- uncomfortable

Key theme: Unsafe

- Unsafe. An invasion of privacy.
- Unsafe and frustratingly powerless to prevent it
- Si, me da inseguridad .

Key theme: Dislike

- intensely dislike *[2 respondents had same response]*

Key theme: Longer responses with multiple feelings

- Horrible! People deserve to feel safe & secure, but when you realize the full extent to which everything about you is just "out there," ready for the highest bidder (or not even!) to receive and exploit, you start spinning....thinking about all of the ways you're now vulnerable, that you didn't even know about, wondering if XYZ happened b/c of 123-data related thing, and not knowing how to protect yourself going forward. And the opt-out options are fraught w/ issues as well: PROVIDING your info in an effort to "protect" it? Absurd. Why would anyone trust that system? It feels like it's all too late and we're all just sitting ducks, zero consequences for those doing the harm, circulating and selling our info--our lives.
- Exploited. Not in control of my life. When everything from location data, to datasets that affect credit score, to employment history....even though I've lived a clean life and have never broken the law, I'm treated like a criminal. I don't know what the data is, but I suspect there's wrong data being sold about me. It causes worse damage than gossip or slander because the data moves faster and... does anyone actually have the ability to remove inaccurate data from the system, including the dark web? No. It's a wicked problem.

Unclear responses

- Not conducive to life
- It makes me feel dangerous.
- I feel like I'm living a transparent life

Data brokers often sell people's highly personal information to law enforcement agencies. How might this impact you and your community? (42 responses)

Key theme: Criminalizing people

- I come from a community that is already disproportionately targeted by the police. Data brokers selling our personal information to law enforcement would endanger our community members even more.
- I am Mexican and American Indian. There is almost no one in my life unlikely to be subjected to abuse by law enforcement on a daily basis, and their access to more info about us than what we look like and where we live, that we're poor people of color in poor neighborhoods, only makes abuse *more* likely. It's terrifying.
- Unfair treatment: Law enforcement agencies may use your personal information for targeted actions or investigations. This can lead to unfair treatment and discrimination, which can negatively impact you and your community.

- My personal information was shared with law enforcement agencies, and I could be the subject of an investigation. Even if I have committed no crime, my personal information may be used to monitor, track or investigate me, which will affect my daily life and work.
- I've never broken the law, but inaccurate data about me, being sold to law enforcement agencies puts me at extreme risk and there's nothing I can do to clean up my record because I'm unaware of what the problem is.
- Law enforcement already targets my communities; them having more information gives them a scary new level of access and avenues for surveillance.
- Due to being involved in progressive social movements I feel at risk of being criminalized or under threat of a possible family separation
- These data brokers undermine the 1st Amendment right to protest and the 4th Amendment protections against unreasonable searches and seizures by selling personal data to the government. Everyone is guilty of something, even if it's going 26 mph (or 24 mph) in a 25 mph zone. Having grown up next to a town where the cops pulled you over for both of those things, I'm aware that such petty offenses may be thrown out of court, but I worry that any such ticket issued in the past 10 years may be permanently logged by data brokers where it can be pulled up and used as a prior offense or evidence for a warrant now.
- As a pregnant person, laws are being passed that criminalize our existence. With the overturning of Roe, highly personal information (buying a pregnancy test at CVS, searching pregnancy symptoms on Google, location data at a Planned Parenthood) may be weaponized for the criminalization of people with certain pregnancy outcomes.
- The data and tools sold to law enforcement have been proven to criminalize communities of color. We already know black immigrants are arrested by local law enforcement at much higher rates than other immigrants. As a result, black immigrants are three times as likely to be deported for criminal convictions. A lot of this is due to data brokers and other surveillance technology which have been proven to exhibit racial bias. We are very concerned that these tools will continue to exacerbate an already unjust and systemically racist immigration system.
- This puts some of my family members at risk of being misidentified due to the prevalence of their names within the already hyper-surveilled Muslim-American community. I know that one incorrect entry could lead to devastating consequences for me or my family members.
- Deportation of the undocumented is an ongoing risk.

Key theme: Distrust and lack of privacy

- This can have negative consequences for individuals and communities, such as a distrust of privacy or an aversion to regulators.
- If law enforcement agencies misuse your personal information, such as using it for malicious surveillance or harassment against you or your community, this can have long-term or even uncontrollable negative effects on you and your community.
- Data brokers selling personal information to law enforcement agencies may lead to privacy violations, which in turn affect their own sense of security and trust. At the same time, others in the community may be exposed to similar risks as a result of this information being leaked.
- Let each other know privacy
- There's no privacy
- It feels like an invasion of my privacy.
- You feel like you're being watched all the time
- The loss of privacy

Other responses

- This will affect our life and may bring danger. *[15 respondents had same response]*

- Causing unnecessary problems for me and my community and seriously interfering with my life. *[4 respondents had same response]*
- It will create more insecurity, separation of families, and low academic outcomes in children and youth due to stress
- I don't know
- uncomfortable

What do you think the CFPB should do to limit the surveillance power of data brokers? (42 responses)

- Prohibit these acts
- Prohibit by law
- Strictly monitor them and do not let them sell information for profit. *[5 respondents had same response]*
- Prohibit not only the sale but also seek penalties and punishments against those who dare to share our data.
- I would love for such corporations to be made illegal. Short of that: 1) Issue policies to govern such agencies and start monitoring them, immediately. 2) Eliminate the "credit header" loophole that currently allows the sale of personal info like DOB, SS#, phone, addresses, and the like. Shameful the loophole even exists. 3) Require these corporations be bound by FCRA privacy laws/protections, for monitoring to begin (see above, don't require US to report something might be going on & then have ad hoc investigations), & for enforcement actions to be brought when violations occur. 4) Require all law enforcement agencies to be bound by these privacy laws/protections--eliminate the loopholes & exceptions for law enforcement that currently exist when it comes to privacy rights.
- Some punitive measures can be formulated.
- Fine them with bigger amounts and strip them of licensing or permitting [to operate in the market].
- Develop and enforce stricter privacy regulations to protect personal privacy information from abuse and disclosure by data brokers.
- The CFPB could issue stricter regulatory standards and regulations to regulate the behavior of data brokers. For example, place restrictions on how data brokers collect, use, and share personal information, force data brokers to disclose their data practices and reveal their data security measures, and improve transparency and accountability.
- The CFPB should forbid the sale of people's personally identifiable information, including address, date of birth, SSN, and phone number, ensure data broker companies are bound by the privacy protections of the Fair Credit Reporting Act, and bring enforcement actions. Privacy protections should be applied to law enforcement, and leaks to law enforcement should be a priority for CFPB enforcement. The CFPB should issue advisory opinions and policies promptly and initiate and publicize enforcement actions now, not after the conclusion of a long regulatory process.
- Issue advisory opinion and policies NOW, don't wait for a long regulatory process. Close "credit header" data loophole that allows sale of people's address, DOB, SSN, phone #. Ensure data broker companies are bound by the privacy protections of FCRA, and bring enforcement actions. Ensure privacy protections apply to law enforcement (no law enforcement exception)
- Require data brokers to delete all data gathered to date. Require data brokers to collect new data only if the consumer affirmatively asks for data to be collected after informed consent - including understanding who the data seller may sell the data to, how long the data collector may keep the data, and how secure the data will be kept. Impose strict liability, with damages, if data brokers collect, store, or sell data without consent. Require data brokers to set up an easy process for a consumer to see what data has been collected on them. Require data brokers to set up an easy process for a consumer to delete any data collected; ensure that such deletion is carried out across

all storage over which the data broker or its affiliated entities control or could control. Explore CFPB's capacity to require companies to comply with the highest relevant standards on privacy and sanctuary. Impose liability on data brokers for harms - including emotional and dignitary harms - caused by their sale or release of data.

- Follow the recommendations/requests of Just Futures Law, MediaJustice, Mijente, the Surveillance Resistance Lab, and the UCLA Center on Race and Digital Justice. In addition, if it wasn't included in their recommendations, automatically opt everyone out of this sort of surveillance. Let data brokers ASK to be let into our lives, and provide services worth the surveillance in exchange. Some people may find it worthwhile (e.g. when they choose the services of Smart Homes),
- Strengthen data privacy regulations: The CFPB can create more stringent regulations and laws to protect consumer privacy and data security. These rules could include requiring data brokers to clearly inform consumers about the type of information they collect, how they use and share the data, and where the data is stored.
- The CFPB should pressure data brokers to allow consumers to opt out of collecting their data without any consequences.
- Restrict them from selling other people's personal information without their consent. *[14 respondents had same response]*
- CFPB or another more appropriate federal agency should become a data clearinghouse. Develop technologies that allow individuals to have complete knowledge of the data sets and inferences being collected about them. Allow individuals to edit inaccurate data, especially related to federally protected classes, and categories protected under civil and human rights law. Editing abilities should have federal oversight, since criminals can also edit their data. OPPOSE legislation that aims to allow individuals to control their data as a new asset class that they can allow access to, because it will create a power imbalance for those of us who wish to avoid being obligated to sell our data.
- I would like to CFPB to give consumers an opportunity to consent to the collection of their information by these data brokers.
- Limit data sharing: The CFPB can limit data brokers' ability to share information in order to protect consumer privacy and security. This includes restricting data brokers from selling or sharing data with third parties, and requiring data brokers to obtain consumer consent before sharing data. *[2 respondents had same response]*
- They should limit the way data brokers can utilize personal data for marketing and advertising. In addition, data brokers have the capacity to re-aggregate data that has supposedly been de-aggregated. They should not be allowed to collect personal information.
- Identify only part of the information
- Reduce intimate questions about the subject
- Appropriate control in appropriate situations
- I don't know

Yes or No Questions (42 responses)

- Do you know what information data brokers have collected on you?
    - Yes: 28
    - No: 14
- Can you tell when a specific data broker has sold your information and to whom?
    - Yes: 8
    - No: 34
- Can you tell when a specific data broker has harmed you?
    - Yes: 15
    - No: 27
- Do you believe it is possible to protect your privacy and security from data brokers?

- Yes: 17
- No: 25

Optional Questions

These questions were optional, so responses do not necessarily add up to 42)

Have you tried to view the data maintained by a data broker on you? (36 responses)

- Yes: 6
- No: 30

Open answer: If yes, please describe your experience. If no, why not? (29 responses)

- I don't know where to look.
- Because it's too much trouble, I don't have time to do it.
- I don't know where to look.
- Visit the websites of Data Protection and privacy organizations, such as the Data Protection Authority, to learn about data protection laws and regulations in your country or territory.
- Oh, my God, this is [too much] trouble, I don't have time to do it.
- I tried to view it and had to go through a third party company who supposedly collects all the data and sends you a list.
- I have not yet because it might lead to the companies collecting more information on me.
- I requested and reviewed the information collected by Facebook and concluded, for myself anyway, that it was more annoying than worrisome. And I don't want to draw attention from organizations with links to organized law enforcement.
- I'm not sure where to start. I haven't looked for a comprehensive list of data brokers.
- No; I already don't understand a lot of the information in my credit report. This sounds like more of the same.
- I don't know where to look.
- I only recently learned about the existence of data brokers, so I know little about the process.
- It doesn't affect me too much.
- Don't know how to query
- I paid Intelius to view my background information. It had accurate and inaccurate data about me, and when I tried to get them to remove it they sent me to their business partner, another paid service (not reviewed by the Better Business Bureau) with a complicated process and a bunch of hoops to jump through. They can't guarantee the cleanup or removal of inaccurate data everywhere on the internet, obviously. So I didn't take action because I realized it wasn't worth it to spend the money and time to deal with them. Here's Intelius' email in response to my request for data removal: We have received your request to have your public data removed from the Intelius website. We care about your privacy and your ability to personally control the display of your public data. The Suppression Center allows you to limit the ability for other users to view your report while preventing others from abusing this function of the website. To exercise this right, access our suppression tool here and click on "Manage Suppression Rules." You will be asked to submit your email address to begin the process. Once you receive an email, you must click "Verify Email" to proceed. This will take you to the "Identity Page", where you will be prompted to provide identifying information to verify your report and validate that you are the person identified in the report. The information you provide will not be sold, shared with third parties, or used for marketing purposes. Upon verifying an email address or phone number, you will receive a unique code via text or email. Enter this code on the "Identity Page" to proceed. Once you have entered all identifying information and verified at least one email or phone number, click "Save" to move to the final step. You can edit and update this information as needed or desired. The final step is to navigate to the "Suppressing Settings" tab. This page will

display all reports corresponding to your validated information. On this page, you can toggle to "Suppress" or "Display" your reports. Please allow up to 48 hours for these changes to reflect on our website. Please keep in mind that we do not remove sex offender location data and that these names could still appear as a possible relative or associate in another individual's background report. Please Note: The Suppression Tool only applies to the publicly available information that is contained in our reports and displayed to consumers on our website. If you want to exercise your CCPA or other state law privacy rights with respect to the user data Intelius collects from you, you can do so here.

Have you tried to remove the data maintained by a data broker on you? (35 responses)

- Yes: 5
- No: 30

Open answer: If yes, please describe your experience. If no, why not? (15 responses)

- I can't find a way []
- I can't find a way []
- Am I crazy? I have to spend time deleting these messages on a regular basis, and I don't have that time.
- I know that even if I delete the message, it will continue to appear, and I have to delete it regularly, which is too much trouble.
- Learn about the data broker's privacy policy, how they collect, use, and share my data, and learn about their data deletion policy.
- I haven't believed that it's possible and I also haven't had the time to try to remove all the data.
- I have not because it might impact my ability to access future resources.
- I'm not sure where to start. I haven't looked for a comprehensive list of data brokers.
- No; it sounds both time consuming and likely to give them more information than I want them to have. If I do it, I'm going to try to remove data from multiple data brokers, not just one.
- I can't find a way or a way.
- See answer above.
- I'm not sure how to do that.
- Don't know how to query
- see above
- I don't know how to do that

Have you tried to correct the data maintained by a data broker on you? (34 responses)

- Yes: 4
- No: 30

Open answer: If yes, please describe your experience. If no, why not? (14 responses)

- I don't know what to do.
- No, I don't even want to check.
- I don't have time for that.
- I don't know what to do.
- I don't know what to do.
- I don't know what to do.
- I'm not sure where to start. I haven't looked for a comprehensive list of data brokers.
- I haven't looked at the information they have on me, aside from the general information in my credit report.
- I don't know what to do.
- I'm not sure how to do that.
- Don't know how to query

- I don’t know what to do.
- see above
- I don’t know how to contact them

Have you taken any other steps to protect your privacy or security as a result of data broker harms? (35 responses)

- Yes: 17
- No: 18

Open answer: If yes, were these steps adequate? If no, why not? (17 responses)

- I can’t do anything about it.
- I try to hide my true information so that no one can guess it.
- I can’t do anything about it.
- I use IP proxy to surf the Internet anonymously to avoid personal information theft.
- I can’t do anything about it.
- I've set privacy settings as high as I can, I’ve opted out of cookie collection wherever possible
- I use IP proxy to surf the Internet anonymously to avoid personal information theft.
- No, I don’t believe so.
- I’ve deleted several social media accounts to try and limit my data online. However, it doesn’t erase the information from my social media accounts when I was younger.
- I try to hide my true information so that no one can guess it.
- I can only assume that my attempts to protect my security/privacy are effective after the last couple of major data breaches at data brokers because I don’t know of any breaches of my personal data. There’s a very good chance that I've just been lucky or haven’t upset people who would want to use my information against me yet.
- I can’t do anything about it.
- I have to give my real name when buying an internet plan, connecting to utilities, and if I ever go to the DMV. I cannot avoid giving away my real information when connecting to vital services.
- I really don’t know how to do it.
- Try not to leave any personal information
- I’ve taken many steps to protect my privacy and security, but they aren’t all a result of data broker harms, per se. Because data brokers’ practices are opaque, and because contacting them and protecting our rights is an extremely time-consuming process, I doubt any consumer can make accurate and verifiable claims about harms done to them. However, there’s a well-documented story about David Carroll, Parsons professor, who requested his data from SCL Group -- the holding company that held Cambridge Analytica. Mr. Carroll spent years trying to get his data from SCL. I recommend you contact him. As far as my own experiences: Some of the organizations and products that are allegedly designed to keep consumers safe are the exact organizations and products perpetrating the crimes. They’re holding the door to our digital homes wide open so criminals can take everything they want. They need to be audited. I paid for NordVPN service and it became a vector for attack. Around the same time, a friend’s instagram account was hacked, the hacked account sent me a DM with a link, I clicked it and then my laptop was hacked. I did a hard reset on the machine and then to keep myself safe I spent a few years using Little Snitch web traffic monitoring software. At first I was very diligent about monitoring the traffic because my system had just been hacked. But then after a while I just started clicking through all of its warnings. Its notifications create too much noise and they don’t do a good job of notifying users about threat level, and clicking through its notifications slows down our access to web content, which is the reason we’re using the internet at all.
- They were not adequate. I try not to use applications and technology. That works but it also has bad side effects because it separates me from society.

Do you believe the government has taken adequate steps to protect your privacy from data brokers? (36 responses)

- Yes: 23
- No: 13

Open answer: If yes, what are those steps? If no, what steps do you believe need to be taken? (12 responses)

- There is already comprehensive consumer privacy legislation.
- The government has introduced consumer privacy legislation to crack down on the sale of information.
- There is already comprehensive consumer privacy legislation.
- The [government] has introduced consumer privacy legislation to crack down on the sale of information.
- The US government has not taken any steps to limit the power and capacity of data brokers to collect data and use data for marketing, advertising, policing and other nefarious purposes.
- Issue advisory opinion and policies NOW, don't wait for a long regulatory process - Close "credit header" data loophole that allows sale of people's address, DOB, SSN, phone # - Ensure data broker companies are bound by the privacy protections of FCRA, and bring enforcement actions - Ensure privacy protections apply to law enforcement (no law enforcement exception)
- Regulate the type of data that can be collected, how long it can be stored, who can access it, what it can be used for. Do not allow quick warrants.
- Some policies have been introduced to protect our interests.
- legal protection
- legislation
- Update the law on data privacy to ban the sharing of data and impose penalties and severe punishments against those who dare to do it
- More severe measures against those who sell data

Do you know what information is collected by data brokers on other people in your community/ies, and how this compares to your data? (34 responses)

- Yes: 10
- No: 24

Open answer: Do you have any concerns about how data brokers' collection of your personal data impacts your communities, and how data brokers' collection of your communities' data impacts you? (11 responses)

- It would affect my life in the community, expose my privacy.
- I am very concerned that the disclosure of my information will cause problems for me and my community and disrupt my life.
- no
- I am deeply connected with families and individuals who have been impacted by deportations. I have been separated from friends, I know and support children who are being raised without one of their parents. These are people who have been picked up because of data sharing from either the state DMV with data brokers or by local judicial system information being collected and supplied to ICE. Data brokers are enhancing a racist and broken system, are contributing to the over-policing of communities of color and immigrant communities, and make our neighborhoods and communities less safe.
- Yes
- I'm worried about how data brokers' collection on women and people they perceive as women for child-bearing purposes may be used to restrict our rights--from health care to traveling to choice

of recreation and food and more--depending on where we're located and how the next election goes. I'm concerned about the information collected on the LGBTQIA+ / Queer community, and just because I don't know what information is being collected doesn't mean I don't find the prospect terrifying. Trans people in particular are already being targeted for genocide as defined by the Geneva Convention in many states. If their information is collected and given to people who wish them ill (which I have no doubt that it all too often is), it has the potential to speed that process. I've seen similar attacks happening in other communities, and to anyone used to looking at the intersections of oppression, it's obvious that people in multiple communities are at more risk. Data brokers are intensifying that risk by making data available to bad actors, certainly within the government and quite possibly outside of it.

- Yes, i think it could be used by some illegal agency.
- Maybe
- Yes, see above
- We are always worried
- I am worried about the youth, I think they are the main victims