COMMENTS OF
THE CENTER ON RACE AND DIGITAL JUSTICE, JUST FUTURES LAW, MEDIA JUSTICE, MIJENTE, AND THE SURVEILLANCE, TECH, AND IMMIGRATION POLICING PROJECT AT THE IMMIGRANT DEFENSE PROJECT, to the
Federal Trade Commission
Trade Regulation Rule on Commercial Surveillance and Data Security
Request for Public Comment

Docket No. 2022-0053
November 21, 2022

By notice published on August 22, 2022 the Federal Trade Commission ("FTC") requests public comment on the prevalence of commercial surveillance and data security practices that harm consumers, and asks whether the Commission should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.[1]

Pursuant to the FTC's notice, the Center on Race and Digital Justice, Just Futures Law, MediaJustice, Mijente, and the Surveillance, Tech, and Immigration Policing Project at the Immigrant Defense Project submit these comments to express strong support for FTC trade regulation rules to protect consumers from commercial surveillance and data practices that harm consumers. Based on years of research and work with impacted communities, we specifically urge the FTC to take action to protect consumers from commercial entities that collect, analyze, monetize, and sell personal data and data analytics products, especially to government law enforcement entities. These higher standards 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.

The 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.

Just Futures Law is a transformational immigration lawyering organization that provides legal support for grassroots organizations engaged in making critical interventions in the United

[1] *Trade Regulation Rule on Commercial Surveillance and Data Security*, 87 Fed. Reg. 51273 (Aug. 22, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.

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, Tech, and Immigration Policing Project of the Immigrant Defense Project (IDP) challenges the growing surveillance state, focusing on ICE policing and migrant control, as well as the rapidly expanding role of technology corporations in local governance. The project supports organizing to build the collective knowledge and political infrastructure to end state violence and to grow a just digital future. See more info here: https://www.immigrantdefenseproject.org/surveillance-tech-immigration-policing/.

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. DHS and ICE use these systems and consumer data to identify, track, detain, and deport people, disproportionately targeting immigrants through these commercial surveillance contracts. The more immigrants comply with U.S. laws, the more they generate digital "paper trails" by getting licenses and insurance, paying bills, sending children to school, filing taxes, working, and participating in society.[2] Commercial entities turn these daily actions into data that exposes people to invasive surveillance and immigration enforcement. Similarly, local police capitalize on commercial surveillance products to target and track racial justice protestors and Muslim communities, ensnaring people in mass policing systems.

[2] Social participation makes people more "findable." The U.S. government encourages immigrants to assimilate, applauding people who perform "model citizenship," but builds systems where people who follow government rules have thick data dossiers that are weaponized by law enforcement. McKenzie Funk, "How ICE Picks Its Targets in the Surveillance Age," *The New York Times* (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

Private companies are the backbone of these surveillance systems, selling products and access to databases that often fall outside the limits of existing government regulations. As the public-private system of data surveillance grows more massive and incorporates more invasive and biased tools from tech corporations, commercial entities and government agencies like ICE and local police increasingly violate people's civil liberties and privacy. The 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.

To protect consumers in the digital policing age, the FTC should limit how companies can access, collect, and use consumers' data, especially when their products are designed for use by law enforcement and other government agencies. We encourage the FTC to also take steps to ensure that commercial surveillance and data collection, especially when linked to government agencies' data programs, are governed by strong accountability and oversight requirements.

This comment focuses on the pervasive use of commercial data products in government surveillance programs and identifies specific data products, types, and practices that should be regulated to prevent harmful, unfair, and discriminatory commercial surveillance practices. **Section I** outlines the harms of dragnet data surveillance, the scope of the commercial surveillance industry, the types of companies we encourage the FTC to regulate, the types of data collected, and examples of harm to consumers, addressing questions 4, 7, 10, and 12 of the ANPR. **Section II** details our recommendations for substantial regulation to limit these harmful data practices, including retention and use of consumer data and the need for transparency in commercial surveillance practices, addressing questions 43, 44, 45, 46, 48, and 83.

Our recommendations urge the FTC to:

1. **Prohibit the operations of data brokers, data analytics, and other predatory companies** that exploit consumers' need for essential services and utilities to capture, repackage, and sell their personal information.

2. **Implement rules to ensure that companies monetizing and building analytics products based on personal data are not violating peoples' civil rights and liberties,** primarily through substantive limits on what data can be collected, how it can be packaged and shared, and when it is deleted.

3. **Create accountability, oversight, transparency, and reporting requirements for private technology and data companies and other commercial entities.** Regulatory mechanisms should hold companies accountable for violating rules and ensure that consumers can understand how their data is being collected and used, delete their data easily, and access a private right of action in cases of harm. Instead of "notice and consent"

that places the burden on consumers, these should focus on accountability and disclosure requirements that reinforce the substantive limits in recommendation #2, and provide the transparency needed for oversight mechanisms to operate.

4. **Prevent the private dragnet surveillance system by prohibiting corporate data broker and data analytics company consolidation and monopoly power in policing data markets.** Like all other tech industries and markets, data brokering markets should be monitored and regulated carefully to prevent data brokers from wielding their monopoly power to sell invasive personal data dossiers to law enforcement, putting the public at risk of biased predictive policing systems and other biased surveillance regimes.

Section I: The Harms of Dragnet Digital Surveillance

Companies are building a dragnet data surveillance web that targets every U.S. consumer.

There is an urgent need to intervene in the sprawling data surveillance market built by data brokers and data analytics companies for explicit use by U.S. local, state, and federal government agencies. Without oversight and intervention, companies that deal in personal data skirt substantive and procedural rules and requirements that protect consumers' civil rights and liberties. Data surveillance has created a booming industry where data brokers and other data analytics companies profit from selling non-consensually collected consumer data to policing agencies and other institutions that make major decisions about people's civil rights and liberties.

This data industry is a purely predatory one that aggressively lobbies to avoid privacy regulations.[3] The industry is designed to benefit data company executives and law enforcement agencies, providing a flood of data collected with little oversight, often using racially-biased algorithms,[4] at the expense of communities already targeted by discriminatory policing. This burgeoning data industry subjects everyone else, including all of the consumers the FTC seeks to protect, to constant, invasive government surveillance, facilitated by third-party data brokers. In essence, data companies collect billions of taxpayer dollars in the form of government contracts, and use that money to strip consumers of their personal privacy.

[3] Alfred Ng & Maddy Varner, "The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress," Markup (Apr. 1, 2021), https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress.

[4] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots," ACLU.org (July 26, 2018), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28; Patrick Grother, Mei Ngan, & Kayee Hanaoka, National Institute of Standards and Technology, U.S. Department of Commerce, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (Dec. 2019), https://doi.org/10.6028/NIST.IR.8280.

Question 4: Why should these companies be regulated?

Question 12: How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?

As the FTC considers how particular types of commercial surveillance harm consumers, it should not limit its regulations to firms working on marketing and advertising technology. It should ensure that trade regulations protecting consumers from ad-tech and other invasive commercial practices also protect consumers from the unfair and deceptive practices carried out by companies in government data and surveillance markets. 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.

Without intervention, 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.[5] Data companies help federal, state, and local governments actively "buy their way around" the constitutional provisions and privacy laws that protect consumers from invasive surveillance.[6] 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.[7] This is, in no small part, because ICE agents dismiss the warrants requirements and other procedural safeguards that protect consumers' rights as pesky, onerous obligations "take too long."[8]

Using privacy data 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. 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 like LexisNexis provide ICE (and other government agencies

[5] Privacy Act of 1974, Pub. L. 93-57, codified at 5 U.S.C. § 552a.
[6] Gilad Edelman, "Can the Government Buy Its Way Around the Fourth Amendment?" *Wired*, (Feb. 11, 2020), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/.
[7] *See* McKenzie Funk, "How ICE Picks Its Targets in the Surveillance Age," *The New York Times Magazine* (Jun. 7, 2021), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[8] Alfred Ng, "Privacy Bill Triggers Lobbying Surge By Data Brokers," *Politico* (Aug. 28, 2022), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.

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.[9] 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.[10]

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,[11] PredPol,[12] and CopLink[13] push our personal data through algorithms and other data-churning systems, creating mosaics of our lives by piecing together billions of datapoints 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.[14] 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.

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. 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. 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 datapoints.[15] 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."[16]

It is difficult to identify precisely how these surveillant and predictive data technologies harm consumers because, due to lack of regulatory oversight and transparency requirements, these

---

[9] Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE," *The Intercept* (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/.

[10] Archana Ahlawat, Ana Ortiz, & Anuj Shah, "The Data Broker to Deportation Pipeline: How Thomson Reuters & LexisNexis Share Utility & Commercial Data with ICE," Just Futures Law and Mijente, https://www.flipsnack.com/justfutures/commercial-and-utility-data-report/full-view.html.

[11] "Gotham: The Operating System for Global Decision Making," Palantir, https://www.palantir.com/platforms/gotham.

[12] "Predpol: the Predictive Policing Company, https://www.predpol.com/.

[13] "Coplink X," ShotSpotter, https://forensiclogic.com/coplink/.

[14] David E. Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act," 115 YALE L. J. 628, 628–79 (2005); McKenzie Funk, "How ICE Picks Its Targets in the Surveillance Age," *The New York Times Magazine* (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

[15] Natasha Lomas, "Researchers Spotlight the Lie of 'Anonymous' Data," *TechCrunch* (Jul. 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

[16] *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/.

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.[17] 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**.[18] Most people who provide their information for cable, phone, and electricity bills have no idea their data–including addresses and Social Security numbers—would be shared this way.[19] 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,[20]** 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 protestors after the murder of George Floyd**, characterizing participants by race, gender, and religion.[21] 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

[17] Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE," *The Intercept* (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/; Sam Biddle, "ICE Searched LexisNexis Database Over 1 Million Times In Just Over Seven Months," *The Intercept* (June 9, 2022), https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/.

[18] Drew Harwell, "Utility giants agree to no longer allow sensitive records to be shared with ICE," *The Washington Post* (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

[19] Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE," *The Intercept* (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/; Sam Biddle, "ICE Searched LexisNexis Database Over 1 Million Times In Just Over Seven Months," *The Intercept* (June 9, 2022), https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/.

[20] John Keegan & Alfred Ng,, "Lawsuit Highlights How Little Control Brokers Have Over Location Data," *The Markup* (Mar. 21, 2022), https://themarkup.org/privacy/2022/03/21/lawsuit-highlights-how-little-control-brokers-have-over-location-data.

[21] Caroline Haskins, "Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location," *BuzzFeed.News* (June 25, 2020), 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), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=6f7c143d4a1e.

surveillance, the **controversial AI company Dataminr helped police monitor nonviolent protests after the murder of George Floyd**, including sharing locations.[22]

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 FTC has the power to regulate. FTC should take up that obligation and create those limits. The agency should explicitly include the firms that sell government surveillance products in their trade regulations, and their regulations should close the transparency and notice loopholes that these companies help third parties including law enforcement exploit. 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.

Question 7: What types of companies should be regulated?

We encourage the FTC to regulate the following commercial surveillance operations, which harm consumers with invasive tracking, data collection, and data sharing and selling to law enforcement agencies often without notice to consumers or their consent. While this list is not exhaustive, these companies include: data brokers, data analytics companies, geospatial and biometric data companies, surveillance technology vendors, biometrics collection companies, and other personal data vendors, especially those that contract with government agencies focused on law enforcement and surveillance. Use of algorithmic analysis, AI, and machine learning in data collection and analysis should also be subject to this higher standard. In addition, companies that both collect and then simultaneously engineer systems to share data broadly should be subject to high levels of scrutiny and limitation.

Consumer data analytics enterprises—including companies that build predictive policing and other "risk" analytics products—regularly violate the rights of consumers, and especially marginalized consumers. Because some of these companies' biggest customers are agencies within the Department of Homeland Security (DHS) and other law enforcement entities, these data companies tend to target BIPOC and immigrant communities. Such surveillance and data analytics products built and sold by private companies are the foundation of some of the most shocking surveillance abuses in modern policing. People ensnared in the dragnet digital policing and surveillance systems built by companies like Venntel, Palantir, RELX Group, Thomson Reuters, and an array of other data brokers, geospatial, biometric collection, surveillance, and data analytics companies. Numerous investigative journalism reports and advocacy campaigns have exposed the

[22] Sam Biddle, "Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr," *The Intercept* (July 9, 2020), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

harms of these companies, like ShotSpotter,[23] Ring,[24] and Clearview AI.[25] Together, these companies construct invasive government surveillance schemes that subject consumers to a host of tracking and targeting schemes.

Question 10: What type of data should be included?

We urge the FTC to regulate any data that's collected on consumers that can be used for the purpose of policing and surveillance, as the commercial practices behind these systems expose consumers and their data to discrimination and harm. We encourage the FTC to identify particular types of data that are most subject to abuse but not to exclusively limit the types regulated, since this can change with technology and commercial use practices. The types of data already subject to abusive and harmful commercial practices include Personal Identifying Information (PII), biometrics, healthcare information and medical records, geospatial and location information, and utility hookups and use data. Data collected for profiling and predictive behavior analysis often forms the backbone of inaccurate and biased data products. Social media and other online activity data is also often collected by controversial web scraping techniques and used in ways that harm consumers.

Section II: Recommendations

The FTC should implement trade regulation rules and take other regulatory action to protect consumers' civil liberties.

The FTC ought to set clear legal requirements to protect all consumers – especially immigrants and Black and Brown people who are most impacted – from these abusive and invasive data surveillance practices. Key actions for federal regulators to take to fulfill this imperative include:

1. Prohibit the operations of data brokers, data analytics, and other predatory companies that exploit consumers' need for essential services and utilities to capture, repackage, and sell their personal information.

Millions of consumers in the United States generate trails of personal data each day by conducting basic activities in their lives, like talking on their cell phone with a loved one, paying a bill to keep the lights on at home, or driving their child to school. The current business model of

[23] Andy Grimm, "Activists call for city to end contract with ShotSpotter," *Chicago Sun-Times* (July 29, 2021), https://chicago.suntimes.com/2021/7/29/22600484/activists-city-end-contract-shotspotter.
[24] Jason Kelley & Matthew Guariglia, "Amazon Ring Must End Its Dangerous Partnerships With Police," Electronic Frontier Foundation (June 10, 2020), https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police.
[25] Just Futures Law, "Fighting Facial Recognition Tech," https://www.justfutureslaw.org/facial-recognition; Louise Matsakis, "Scraping the Web Is a Powerful Tool. Clearview AI Abused It," *Wired* (Jan. 25, 2020), https://www.wired.com/story/clearview-ai-scraping-web/.

data brokers, data analytics, and other predatory companies functions by amassing gigantic troves of these digital breadcrumbs without the knowledge or consent of most consumers, digesting that data with racially-biased algorithms, and then selling it to government agencies that use the data to conduct mass surveillance of the U.S. population, flouting the civil liberties we hold dear and disparately harming Black, Brown, and immigrant communities.

The dossiers of information furnished by these companies are used to target, arrest, jail, and deport hundreds of thousands of people each year, tearing families apart and exposing them to mortal violence. These unscrupulous companies currently reap millions in profits – profits funded by taxpayers – by assisting their government partners in circumventing legal restrictions against spying on private individuals. This industry cannot be allowed to continue to profit from the flagrant abuse of marginalized communities.

2. Implement rules to ensure that companies monetizing and building analytics products based on personal data are not violating peoples' civil rights and liberties, primarily through substantive limits on what data can be collected, how it can be shared, and when it is deleted.

Concrete and substantive limitations to prevent unfair data practices and protect civil right and civil liberties should include but are not limited to:

- Limiting the types of data that can be collected, analyzed, and sold by commercial entities, referencing our answer to Question 10 above, including regulation of the sharing and sale of these types of data

- Prohibiting private companies from incorporating utility data and other data collected on an involuntary basis (or in exchange for necessary goods and services) into digital surveillance and digital analytics-based risk assessment schemes and products, particularly when used by government agencies including law enforcement

- Limiting private companies from collecting, licensing, incorporating, and using geolocation, biometric, and other sensitive data in "risk management" and other products used for policing and surveillance purposes without properly following constitutional due process requirements

- Prohibiting private companies from using web scraping technologies or services to gather and compile personal data

- Ensuring that consumers' personal data that is collected or licensed by commercial entities, especially when shared with government and law enforcement agencies, complies with pre-set limits on retention and data minimization

- Prohibiting data sharing, data profiling systems, and other types of data tools for use in warrantless, non-particularized surveillance and policing programs and operations

3. Create accountability, oversight, transparency, and reporting requirements for private technology and data companies and other commercial entities.

Regulatory mechanisms should hold companies accountable for violating rules and ensure that consumers can understand how their data is being collected and used, delete their data easily, and access a private right of action in cases of harm. Instead of "notice and consent" that places the burden on consumers, these should focus on accountability and disclosure requirements that reinforce the substantive limits in recommendation #2, and provide the transparency needed for oversight mechanisms to operate.

These requirements for data brokers, data analytics companies, and other commercial entities should include:

a. Requiring companies to be transparent and disclose to consumers and the public what data they are collecting, what the sources of the data are, how it is used, who it is shared with, and how long they retain the data. These requirements must also include clear and accessible ways for consumers to delete their data and prohibit its use and sharing.

Data companies should be required to tell consumers what data they are collecting, what the sources of their data are, and how they are using the data. They should also be required to tell consumers who they are selling data to or sharing it with, including when they are sharing data to comply with warrants and subpoenas. The data companies should also be required to have records management policies like those in the Privacy Act of 1974, which ensures that the public will receive public notice when the government collects personal data. Per the Privacy Act, before an agency can collect people's personal data, they must tell the public why they are going to use the data, set clear limits on data use and retention, and allow the public to opt in to the data collection scheme. The Privacy Act's requirements were enacted by Congress to prevent the invasive, secretive, and unlimited data surveillance that data brokers and data analytics companies are building with government agencies.

Alone, this recommendation is not enough, as it places the burden on consumers and does little to prevent abuses as it does not necessarily change how data is used. It must be combined with substantive limits in recommendation #2 in order to prevent harm to consumers.

b. Mandating that data brokers and data analytics companies provide regular, in-depth reporting about how they are collecting, using, and maintaining consumer data collections and promptly notify the FTC and consumers of changes to those collections, uses, and maintenance practices.

The Privacy Act and other public notice and transparency laws and rights were also meant to prevent secret dragnet policing schemes like those that dominate modern law enforcement regimes. Right now, the data companies that work with the government have no reporting or oversight obligations. In some cases, data companies even insert non-disclosure language into their government contracts that prevent agencies from even naming their company or its products on press releases and promotional materials.[26] These types of disclosures are often the only way that journalists and the public know that the companies' products are being used without filing FOIA requests or conducting other in-depth investigations.

Journalists and the public should not have to file burdensome, time-consuming FOIA requests to see how the government is working with data brokers and other data analytics companies, only to receive very limited information from the government. The signatories of this letter, alone, have collectively spent thousands of hours and an overwhelming amount of effort and expense to pursue FOIA requests in efforts to piece together the information necessary to understand how these systems affect our community members. Without explicit transparency regulation requiring otherwise, these companies hide their surveillance work from consumers. They are not considered state actors, despite their central roles in government surveillance, so they do not currently have to comply with procedural due process requirements or procedural requirements created by Congress in laws like the Privacy Act of 1974.[27] This allows these commercial entities to continue their harmful practices.

For the sake of consumer protection, it is vital that these companies transparently disclose information about how they are using all of our data, especially for surveillance and policing programs. Consumers deserve to know how their data is being collected, monetized, shared with, and used by government agencies to surveil them. The lack of transparency requirements means that even though data companies make millions of dollars aggregating and providing invasive personal dossiers to agencies like ICE, consumers know little (if anything) about what the companies are collecting and what they are doing with their data.

4. Ensuring through regulatory oversight and enforcement mechanisms that companies are using data in ways that comply with data protection laws and constitutional requirements, especially in situations where the companies are working with government entities.

Oversight and enforcement is necessary, in conjunction with reporting and transparency requirements, to limit harm to consumers. There must be accountability mechanisms, within the

[26] Devin Coldewey, "Records Show ICE Uses LexisNexis to Check Millions, Far More than Previously Thought," *TechCrunch* (Jun. 9, 2022), https://techcrunch.com/2022/06/09/records-show-ice-uses-lexisnexis-to-check-millions-far-more-than-previously-thought/.

[27] Nathaniel Kim, "The Impact of Public-Private Data Sharing on Law Enforcement," *Georgetown Law Technology Review* (Apr. 2022), https://georgetownlawtechreview.org/the-impact-of-public-private-data-sharing-on-law-enforcement/GLTR-04-2022/.

FTC's scope, to ensure that corporations that violate substantive limitations and rules cannot continue their harms to consumers. The FTC has already practiced algorithmic disgorgement in its March 4, 2022 settlement against Weight Watchers.[28] Such practices should also be applied to disgorgement of datasets from data brokers when FTC investigations find that data brokers have broken substantive limitations and rules. When appropriate, the FTC should levy its criminal liaison unit to work with prosecutors to bring criminal consumer fraud cases against data brokers and other companies in the commercial surveillance industry.

Additionally, we urge the FTC to consider creating a separate reparations fund when fines, fees, or penalties are levied against companies that are found to have broken data protection laws and constitutional requirements. In order for companies to be sufficiently incentivized to follow the law, penalties must be extensive enough that they amount to more than "the cost of doing business." Given the different sizes of companies and their profits, we recommend that the FTC use percentages of profits or revenues rather than flat, singular, universal amounts when setting what monetary penalties companies will face if they break the law.

a. Creating a private right of action that allows consumers to seek redress for the improper collection, use, and exploitation of their data.

Like other laws governing private industries that pose significant risks to the public, data privacy laws and regulations should provide mechanisms that allow consumers to prevent dangerous data uses and to intervene when their data is being exploited. People have the right to use legal mechanisms to stop state actors from violating their constitutional rights, including their Fourth Amendment rights protecting them from warrantless searches and seizures. They should be able to use legal mechanisms to stop the private companies that work hand-in-hand with the government from doing the same types of invasive practices.

When industries grow so powerful that they can significantly impact consumers' access to life, liberty, and property, the government has granted consumers the right to seek legal redress. Private rights of action built into environmental laws and consumer protection measures help level the playing field between industries that pose risks to the public. By explicitly including private rights of action in consumer protection laws, the government has recognized that companies have the power to impact access to safe drinking water and non-toxic food products need an additional layer of accountability to consumers. The government should create similar provisions for consumers in the laws and regulations that govern data companies.

[28] "FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data," Federal Trade Commission (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive.

4. Prevent the private dragnet surveillance system by prohibiting corporate data broker and data analytics company consolidation and monopoly power in policing data markets.

Government data brokering markets should not be able to wield their monopoly power to sell invasive personal data dossiers to law enforcement. Companies that dominate information markets have outsized power to gather, collect, and control massive data dossiers of consumers' data. Because information, including personal data, is non-fungible (each piece is unique), data brokers compete to get as much personal information from as many sources as possible. In order to be an industry-leading data broker, you must have larger data collections than your competitors. The firm with the most data can overtake its rivals. This competition to collect more invasive data makes personal data market monopolies especially dangerous to consumers. The companies gather larger quantities of more invasive data to "win" the market. Because the companies are voracious data collectors, it is almost impossible for people to escape their data collection practices.

Without adequate data privacy protections, and with the companies' data market dominance, data broker monopolists make it impossible for consumers to control how their data is used, or to escape data policing and surveillance. The FTC should intervene to stop data brokers from leveraging their market dominance to create all-encompassing consumer policing products that exploit consumers' inability to opt out of, or avoid, data collection. Allowing data brokers to consolidate market power forces consumers to be the subjects of biased predictive policing systems and other biased surveillance regimes.

Conclusion

Faced with the growing power of the commercial surveillance industry and its coordinated and widespread abuse of consumers, the Federal Trade Commission must take effective action to rein in the industry. We ask the agency to issue regulations that reach the broad range of companies undertaking commercial surveillance activities, that protect against the exploitation of consumers in Black, Brown, and immigrant communities by imposing substantive limits on the collection, analysis, use, sharing, selling, and retention of data, that mandate companies to produce regular reports and disclosures on their use of personal data, and that provide an avenue for consumers to seek redress in court when commercial surveillance companies violate their rights. We ask this as the bare minimum toward our ultimate goal of abolishing surveillance and achieving data liberation. We look forward to the FTC implementing these recommendations and are available to discuss them in further detail.