Consumer Financial Protection Bureau

August 15, 2023

PROTECTING THE PUBLIC FROM DATA BROKERS IN THE SURVEILLANCE INDUSTRY

The surveillance industry tracks, collects, and monetizes information about people. Many of these firms assemble data to feed "artificial intelligence" (AI) that makes decisions about our daily lives. After conducting a public inquiry into data brokers and assessing today's uses of AI that are often powered by data from the surveillance industry, the Consumer Financial Protection Bureau (CFPB) will be issuing proposed rules under the Fair Credit Reporting Act (FCRA) to address business practices used by companies that assemble and monetize our data. The CFPB is now inviting small businesses to contact the agency if they are interested in providing feedback prior to the issuance of a proposed rule.

BACKGROUND

- **In 1970, Congress enacted the Fair Credit Reporting Act (FCRA), one of the first data privacy laws in the world, to regulate this market.** Before passing the FCRA, Congress investigated the growing data surveillance industry and found that, while data brokers had assumed a vital role in assembling and evaluating consumer credit and other information on consumers to meet the needs of commerce, there was a need to ensure that they acted fairly, impartially, and confidentially.

- **The FCRA was designed to strictly regulate and constrain the monetization of people's personal data.** Congress grew alarmed that companies had begun collecting information about people's financial status, bill-paying records, arrests, judgements, suits, and other sensitive information on a wide-reaching scale, and that individual lawsuits to protect people's privacy and identity under common law were not providing enough public regulation and supervision of the emerging industry.

- **The FCRA limits how data from data brokers can be used.** The law strictly prohibits selling and using consumer report data unless it is for one of the few authorized "permissible purposes." In addition, people have a right to request their data, be told when someone uses it to make adverse decisions about them, and dispute their data. There are also a number of protections designed to prevent false reporting. The law is enforced by a coalition of government enforcers, and consumers have a right to sue under the FCRA.

- **Since the FCRA's enactment in 1970, advances in technology have created new ways to harvest data from individuals, especially online.** For example, companies using business models that rely on newer technologies and novel methods to collect and sell consumer data have emerged and evolved with the growth of the internet and advanced technology, leading to even more invasive surveillance practices. But while the technology has changed, and the market has grown, it is still fundamentally the same business and the rights created by Congress are still relevant today.

THE CFPB'S FORTHCOMING PROPOSAL

- **The CFPB plans to propose rules that would ensure that the public is protected from modern-day data brokers.** Forthcoming proposals will be designed to ensure that companies, including data brokers, comply with the FCRA. This would mean that firms that monetize certain data would be prohibited from selling it for purposes other than those authorized under the FCRA. A set of fundamental rights will provide essential protections to consumers, including the right to obtain their data and dispute inaccuracies.

- **The proposals under consideration would provide that a data broker or other company in the surveillance industry can be covered under the FCRA in a variety of ways, including if they sell certain types of consumer data.** Under such a proposal, a company's sale of data regarding, for example, a consumer's payment history, income, or criminal records would generally be a consumer report.

- **Additionally, the proposals under consideration would clarify the extent to which "credit header data" constitutes a consumer report.** This would reduce the ability of credit reporting companies to impermissibly disclose sensitive contact information that can be used to identify people who don't wish to be contacted, such as domestic violence survivors. Credit header data is personally identifying information like someone's name, address, or Social Security number, which is held by traditional credit bureaus. Much of the existing data broker market relies on credit header data purchased from the big three credit bureaus to create their individual dossiers.

- **As a consequence, it would generally not be legal to sell this kind of data for a reason other than a "permissible purpose."** Credit header data could be sold for purposes like credit underwriting, employment applications, insurance underwriting, and government benefits applications, but not, for example, for targeted advertising, to train AI, to

sharpen chatbots or similar AI services, or to individuals who could be stalkers or perpetrators of domestic violence.

THE CFPB'S PUBLIC INQUIRY INTO DATA BROKERS

- **In March 2023, the CFPB launched a public inquiry regarding data brokers.** A request for information sought public input about people's experiences with these companies and their business practices. Data brokers, firms that collect, aggregate, sell, resell, license, or otherwise share consumers' personal information, include first-party data brokers that interact with consumers directly, as well as third-party data brokers with whom the consumer does not have a direct relationship. Many of the more than 7,000 responses echo the same concerns raised by Congress that the FCRA was originally designed to address.

- **Commenters focused on protecting sensitive information:**

    - **Experts reported that data brokers are selling highly sensitive information.** For example, they are selling data about members of the U.S. military that include financial information, including estimated income, net worth, home value, and credit rating. Experts also expressed concern about the collection and sale of lists of people with mental and physical health conditions, those that have unmanageable debt, and those who are single parents.

    - **Commenters highlighted that data broker harms impact some more than others.** The people most at risk from many data broker harms include people who are elderly, have dementia, or are pregnant; low-income families struggling to access housing, food, or medical care; people of color; limited English proficiency individuals; immigrants; LGBTQI+ individuals; military families; survivors of intimate partner violence; and children and teens.

    - **Commenters pointed out that data is being shared in ways that consumers would not expect.** For example, commenters noted data was being shared from consumers' vehicles, or apps that collect their health data. They shared concerns that deidentification may not work, and that people can be easily re-identified from aggregated, anonymized data. Compounding these issues, inaccuracies in the data broker system can cause substantial harm, and commenters cited numerous examples of such inaccuracies.

- **Commenters called for more accountability.** The responses highlighted the lack of oversight of the data broker industry and called for action. Individuals overwhelmingly expressed their frustration at the lack of control and privacy they have with regard to their data, and the harms that result—from unwanted spam emails, calls and texts, to being targeted for scams and identity theft, and even threats to one's physical safety and security. Because of the vast amount of information they hold, data brokers too often are the source of harmful data breaches that impact Americans.

- **People warned about AI applications.** Commenters noted that the availability of highly granular data from data brokers, when combined with advanced technology like AI, can create a risky environment where surgically precise scams and fraud can flourish at scale.

OTHER RECENT CFPB ACTIONS RELATING TO CREDIT REPORTING

The CFPB collects consumer complaints, enforces the FCRA and the prohibition against unfair, deceptive, or abusive acts or practices against consumer reporting companies, and conducts confidential exams.

- **The industry has consistently been a major source of consumer complaints.** In fact, credit or consumer reporting has been the most-complained-about product to the CFPB every year since 2017. Complaints about credit or consumer reporting represented roughly 76 percent of consumer complaints submitted to the CFPB during 2022, far more than any other category of consumer product.

- **The CFPB has taken a number of recent actions to address problems in the surveillance industry.** Since 2021, the CFPB has taken a number of relevant actions. In November 2021, the CFPB issued an advisory opinion making clear that it is illegal to use sloppy identity matching practices that result in false data. In July 2022, the CFPB issued an advisory opinion to reaffirm the FCRA's confidentiality requirements, making clear it is illegal to provide data on the wrong person. In August 2022, the CFPB issued guidance making clear it is often a violation of the prohibition on unfair acts or practices to have insufficient data protection or security for sensitive consumer data. In October 2022, the CFPB issued additional guidance making clear it is illegal to report facially false junk data on consumers. And in November 2022, the CFPB issued guidance making clear that consumer reporting companies need to take consumers' dispute rights more seriously.

- **The CFPB sued one of the biggest credit reporting companies for repeatedly breaking the law.** In April 2022, the CFPB sued TransUnion, alleging the company used digital dark patterns to dupe Americans into subscription plans, and for repeatedly violating the law and prior enforcement orders.

NEXT STEPS

There are many initiatives at the state and federal level, including by the Federal Trade Commission, to address modern-day surveillance practices. The CFPB is developing its proposed rules to work in coordination with other laws and regulations.

For certain regulations, the CFPB—along with the Office of Advocacy in the Small Business Administration and the Office of Information and Regulatory Affairs in the Office of Management and Budget—convenes a Small Business Review Panel under the Small Business Regulatory Enforcement Fairness Act to receive feedback from small business panelists. Before the panel meets, the CFPB sends panelists an outline of the proposals under consideration, and the CFPB publishes that outline for the public. After receiving feedback from the small entity panelists, the CFPB will issue a report summarizing the feedback.

Following that report, the CFPB issues a notice of proposed rulemaking, which gives the broader public an opportunity to comment on a proposed rule. After considering those comments, the CFPB may make changes to the proposed rule before issuing a final rule.

Small businesses interested in participating as a panelist should contact the CFPB within the next week at CFPB_consumerreporting_rulemaking@cfpb.gov.