Consumer Financial Protection Bureau

Fact Sheet: The CFPB's Proposed Rule to Rein in Sprawling Data Broker Industry

In today's economy, personal information about consumers is frequently revealed and collected during routine activities, from ordering products online to downloading apps or swiping credit cards at stores. A growing industry of "data brokers" has emerged to collect and sell a wide range of information about consumers, often without their consent. The CFPB's proposed rule would help ensure that data brokers comply with the Fair Credit Reporting Act, a major federal privacy law. The rule would strengthen accountability for data brokers, making sure that certain financial data, like consumers' income, is only shared for legitimate purposes and restricting credit bureaus from selling people's sensitive information, like Social Security numbers and phone numbers.

Data brokers: a growing industry that traffics in sensitive consumer data

Data brokers are companies that collect, aggregate, sell, resell, license, enable the use of, or otherwise share consumers' information. They gather information about credit, criminal, employment, and rental histories of hundreds of millions of Americans, along with other sensitive information.

Types and sources of information collected by data brokers

Data brokers obtain information from a variety of sources, including retailers, websites and apps, newspaper and magazine publishers, and financial service providers, as well as cookies and similar technologies that gather information about consumers' online activities. Other information is publicly available, such as criminal and civil record information maintained by federal, state, and local courts and governments, and information available on the internet, including information posted by consumers on social media.

Much of the information compiled by data brokers is private and highly sensitive. This may include information about a consumer's finances, income, physical and mental health, sexual orientation, religious affiliation, and political preferences, as well as information about the websites and apps the consumer visits or uses, the stores the consumer frequents, the products the consumer buys, and the consumer's location throughout the day.

The volume of data collected, bought, and sold by data brokers is enormous. Technological advancements have also made it increasingly feasible to re-identify consumers in datasets that have otherwise been de-identified, and at times even identify consumers from aggregated data.

How information is sold and used

Data brokers analyze and package consumers' information into reports used by creditors, insurers, landlords, employers, and others to make decisions about consumers. Data brokers may also use information about consumers, or inferences they have drawn from that information, to create elaborate dossiers about consumers to be used to target marketing activities.

Risks to national security, financial wellbeing, and personal safety

The proliferation of sensitive information exchanged in the data broker marketplace, often without consumers' knowledge or consent, harms consumer privacy. Inaccurate information can cause consumers to be denied access to products, services, or opportunities that they would have qualified for had the information been accurate. Sensitive consumer information can be used to target certain consumers for identity theft, fraud, or predatory scams, or other harmful purposes.

National security and foreign surveillance risks

Foreign adversaries can purchase detailed personal information about military service members, veterans, government employees, and other Americans for pennies per person. National security experts have issued warnings about the risks of the unchecked sale of sensitive contact information and financial data.

Duke University researchers were able to purchase individually identified information about active-duty military members' income, net worth, and credit rating, as well as sensitive contact information, which can be used for purposes of coercion, blackmail, or espionage in order to obtain military or other classified information, threatening national security.

For example, information about someone's level of indebtedness could easily be exploited by countries of concern, like China, to blackmail or compromise members of the military who have classified information in ways that put our national security at risk. Foreign governments have actively sought to acquire this type of information in the past. In 2020, DOJ charged four members of the Chinese People's Liberation Army with orchestrating the operation at Equifax to obtain personal data on 145 million Americans. The easy availability of contact information of servicemembers or people who have access to infrastructure that is important for national security, like the electric grid or cyber infrastructure, makes it easier to target or conduct phishing attacks to gain access to those assets.

Data brokers can facilitate the targeting of individuals by allowing entities to purchase lists that match multiple categories, like "Intelligence and Counterterrorism," "substance abuse," "heavy drinker," or even "behind on bills." This enables the creation of detailed dossiers for potential espionage,

surveillance, or blackmail operations, allowing relatively small investments to be leveraged into mass surveillance operations.

Criminal exploitation by scammers

Identity thieves and scammers purchase detailed financial profiles to target vulnerable consumers, particularly seniors and financially distressed individuals. For example, fraudsters can obtain from data brokers lists of people with income below a certain threshold. Thieves also can obtain information from data brokers that enables them to steal people's identities and open new accounts or drain existing ones. These criminals can use this data to execute sophisticated fraud schemes and steal retirement savings, often targeting Americans who can least afford the losses.

Elder fraud is a significant subcategory of fraud that can be facilitated by the unauthorized use of contact information. The FBI's Internet Crime Complaint Center (IC3) reported that call center schemes overwhelmingly target older adults and consumers over the age of 60 lost more to these scams than any other age group. To the extent that financial fraud and identity theft is facilitated by the sale of personal identifiers collected by consumer reporting agencies, the CFPB expects that the proposed rule would reduce unauthorized access by fraudsters.

Violence, stalking, and personal safety threats to law enforcement personnel and domestic violence survivors

The availability of sensitive contact information poses risks to those who are targeted for their profession, such as judges, police officers, prosecutors, government employees, and other members of the law enforcement community. Several states have already had to take action to protect judges and law enforcement officers after violent incidents, including the 2020 murder of a federal judge's son by an attacker who purchased her home address.

Additionally, it is possible to pair individuals' contact information with information from other datasets to identify and track individuals, including those in law enforcement or working undercover. For instance, journalists at the New York Times in 2019 demonstrated how a similar approach could be used to identify U.S. Secret Service agents working on President Trump's detail.

Domestic violence survivors also face grave dangers when their current addresses and phone numbers are readily available for purchase through data brokers. A study by the National Network to End Domestic Violence found that over half of victim service agencies surveyed reported that they work with victims whose stalker used public information gathered from data brokers online to stalk them, and previous court cases have documented how a stalker can use data broker services to locate and harm their victims.

Predatory marketing and data misuse

Data brokers sell lists of financially vulnerable individuals to predatory lenders for targeted marketing campaigns. This practice is compounded by the widespread sale of personal identifiers collected by consumer reporting agencies, also known as "credit header" data—including names, addresses, and Social Security numbers—which has created a thriving market for sensitive personal information that puts Americans' privacy and financial security at risk.

Data brokers have marketed financial-related lists including those with names such as "Bad Credit – Card Declines," "Paycheck to Paycheck Consumers," "Suffering Seniors," "Cash Cows – Underbanked File," and "Bankruptcy Filers," among others. The information in these lists can be used to pitch predatory and unlawful products to families in financial distress.

The Fair Credit Reporting Act: a landmark privacy law

The Fair Credit Reporting Act (FCRA), one of the first data privacy laws in the world, was passed by Congress in 1970 to address the growing data surveillance industry. Credit reporting companies were largely unchecked, and consumers were often powerless to protect themselves from harms. Congress enacted the FCRA to protect consumers' privacy by restricting the communication of personal information by consumer reporting agencies (CRAs).

Limits on how consumer information may be used

The FCRA imposes clear bright-line rules permitting people to obtain consumer reports from consumer reporting agencies only for certain specified purposes, known as *permissible purposes*. These purposes include evaluating a consumer's eligibility for credit, insurance, employment, and other purposes listed in section 604 of the law. The FCRA generally forbids consumer reporting agencies from furnishing consumer reports to users who lack a permissible purpose.

Consumers' rights to access reports and dispute inaccurate information

Consumers have various rights under the FCRA, such as the right to dispute the accuracy of information in their file and to be notified when, for example, a creditor, landlord, or employer relies on consumer report information to make a negative decision about the consumer's application for credit, housing, or employment. In response to a consumer dispute, consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information, and may not report outdated negative information.

Ensuring that data brokers comply with the FCRA

Many data brokers attempt to avoid liability under the FCRA by arguing that they are not consumer reporting agencies selling consumer reports. Consequently, they do not treat the consumer information they sell as subject to the requirements of the FCRA, even though they collect, assemble, evaluate, and

sell the same information as other consumer reporting agencies—and even though their activities pose the same risks to consumers that motivated the FCRA's passage.

Treating data brokers as consumer reporting agencies

Companies like the nationwide consumer reporting agencies (Equifax, TransUnion, and Experian) and others are data brokers that are currently covered under the FCRA. The CFPB's proposal would address the circumstances under which data brokers and their activities are covered by the FCRA.

The proposed rule clarifies the definition of consumer report. First, the rule proposes that a data broker that sells any of four types of information about consumers—a consumer's credit history, credit score, debt payments, or income or financial tier—generally is selling a consumer report. Second, the rule proposes that when a data broker communicates consumer information for any reason, if a person receiving the information then uses the information for an FCRA purpose, the communication would be a consumer report. A data broker that sells consumer reports generally would be a CRA under the FCRA.

Limiting how personal identifiers may be used and shared

Under the proposed rule, communications from consumer reporting agencies of certain personal identifiers that they collected to prepare a consumer report—such as name, addresses, date of birth, Social Security numbers, and phone numbers—generally would be consumer reports. This would mean that consumer reporting agencies could only sell such information—so-called "credit header" data—if the user had a permissible purpose under the FCRA.

Restricting marketing uses of consumer reports

The proposal emphasizes that marketing is not a "legitimate business need" under the FCRA. Under the proposal, CRAs could not use consumer reports to decide for an advertiser which consumers should receive ads and would not be able to send ads to consumers on an advertiser's behalf.

Requiring clear consent for data sharing

One of the FCRA's permissible purposes is related to consumer consent. The CFPB is concerned that some CRAs and users rely on broad and vague consumer authorizations to furnish and obtain consumer reports under this permissible purpose. The proposed rule would require that, for this permissible purpose to apply, consumers must be provided a clear and conspicuous disclosure stating how their consumer report will be used. It would limit how such reports could be procured, used, and retained, and it would require that consumers have a right to revoke their consent.