Mounting Focus on Data Brokers: Is More Regulation Coming?

August 24, 2023

During the past year, there's been a flurry of regulatory activity related to data brokers. Whether in Congress or state legislatures, at federal agencies or the White House, many policymakers are pushing in the direction of increased regulation. For those not following this issue closely, here's a snapshot of some key developments, starting with some history:

Background on Data Broker Regulation

The debate surrounding data brokers and regulation isn't new. For decades, policymakers and enforcers have raised concerns about the collection and sale of consumer data by these entities, citing the sensitive nature of the information and profiles that they sell, the use of this data in making consequential decisions about consumers, and the invisibility of most data brokers to the public. (See, e.g., here, here, and here.)

In the 1970s, Congress passed the Fair Credit Reporting Act (the nation's first commercial privacy law) to regulate consumer reporting agencies (CRAs), an important subset of these entities. The FCRA sets forth data privacy and accuracy requirements when CRAs sell (and companies furnish and use) consumer data for decisions affecting people's eligibility for credit, jobs, and insurance. The FCRA didn't end the debate, however. Since then, some policymakers have pressed for broader regulation of data brokers, especially with the advent of mobile devices and other technological advances, enabling data brokers to collect more detailed data about consumers, and to make more granular inferences and predictions, and then sell this information to the public. In response, data brokers have pointed to the beneficial services they provide, and have argued that existing laws (including the FCRA, the Gramm Leach Bliley Act, the FTC Act, and now numerous state privacy laws) are adequate to address any harms that occur.

Recently, this debate has accelerated, as shown by the increased regulatory activity we are seeing today. For some policymakers, the repeal of *Roe v. Wade* and its implications for reproductive privacy has added an important new dimension to the debate. On April 15, the White House convened a roundtable of government officials, academics, advocates, and other experts to discuss "harmful data broker practices" and provide further impetus for regulation.

Congress

So, what specific proposals are we seeing? Not surprisingly, some of them are coming from Congress. In July, we blogged about two bipartisan efforts to stop the government from purchasing consumers' location and web browsing and search history from data brokers, absent a warrant or other due process measures. One of these proposals (an amendment to the House National Defense Authority Act bill) would restrict such purchases by DOD. Another (the *Fourth Amendment is Not for Sale Act*, now introduced in both the House and the Senate) would restrict such purchases more

broadly across the federal government. All of these bills are pending, with Congress now in recess.

Readers also may recall that the leading federal privacy bill (the bipartisan American Data Privacy and Protection Act) contains strict data broker provisions requiring online registration and a one-stop mechanism allowing consumers to delete data held by data brokers and prevent further collection by these entities. Other recent federal bills (e.g., the bipartisan DELETE Act) contain even stricter data broker requirements.

Federal Trade Commission

The FTC is also very active in this area. In a 2022 blogpost, an FTC official warned that the FTC will use the "full scope of its authorities" to stop the "illegal use and sharing" of consumers' location, health, and other sensitive data. Soon after, the FTC filed a lawsuit against data broker Kochava, alleging that its sale of location data obtained from mobile devices harms consumers and is legally "unfair" because the data can reveal sensitive locations that consumers visit, such as reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. In addition, the ANPR in the FTC's Commercial Surveillance and Data Security Rulemaking is replete with references to data brokers and data sales, suggesting that this could be a focus of any rule it proposes.

Like Congressional efforts, the FTC's actions here are pending. In *Kochava*, the court dismissed the FTC's initial complaint due to what it viewed as the hypothetical nature of the FTC's injury allegations, but the FTC has filed a new complaint (under seal). In the FTC's rulemaking, the comment period for the ANPR closed last November, so the FTC could release a proposed rule any day now. We await news on both fronts.

California – SB 362

No privacy discussion would be complete without California. And sure enough, the California legislature is currently considering new data broker legislation. In brief, SB 362 would amend the state's existing data broker law by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information. This would in turn trigger a ban on further data collection by these entities, unless consumers opt in. The law also would allow an "authorized agent" to request deletion for the consumer, require independent compliance audits every three years, and mandate regular reports to the public and to the California Consumer Protection Agency. Due to the broad definition of "data broker," the bill would cover a wide array of entities, including members of the advertising industry.

If passed, this law would substantially up the ante for data brokers operating in California, and could spread to other states. Currently, eleven states have enacted comprehensive baseline privacy laws, but only a few have data broker laws, with mostly modest requirements. Not surprisingly, opposition to the bill is strong in the data broker and ad industries, who (according to news reports) say it will hurt anti-fraud efforts and the economy, and have launched an effort to defeat the bill. Because California's legislature adjourns September 14, the window for action is closing soon.

Consumer Financial Protection Bureau

Finally, in what could be the most consequential data broker regulation of all, CFPB Director Rohit Chopra just announced (on the day of the White House roundtable) that the CFPB will soon launch a rulemaking to "modernize" the FCRA so that it reflects how today's data brokers "build even more complex profiles about our searches, our clicks, our payments, and our locations" and

“impermissibly disclose sensitive contact information” of people who don’t want to be contacted, such as domestic violence survivors.

Among other things, per Director Chopra, the CFPB is considering proposals to bring within the FCRA (1) a data broker’s sale of certain types of data (e.g., payment history, income, criminal records) because the data is “typically” used to make credit, employment, or certain other eligibility determinations and (2) credit header information, a major source of information for data brokers that has long been considered to fall outside the FCRA. Such proposals would dramatically extend the FCRA’s reach to a broader class of data brokers than are currently covered. According to Director Chopra, the CFPB will publish an outline of proposals and alternatives next month.

* * *

All of the above proposals are now pending, so it’s not clear whether they will reach fruition or what shape they will ultimately take. However, the sheer volume of activity shows that data brokers are in the spotlight and are likely to remain there for a while