Why Data Brokers Need Federal Regulation

Sofia Hernandez

Department of English, El Paso Community College

ENGL 1301: Composition I

Professor Wood

December 12, 2025

Why Data Brokers Need Federal Regulation

Every time you unlock your phone, click on a website, or scan your loyalty card at the store, you are giving away little pieces of information about yourself. These digital breadcrumbs tell a story about who you are, but you are not the one telling it. Companies you have probably never heard of, called data brokers, are collecting these pieces, putting them together into detailed profiles about you, and selling your life story to whoever will pay for it. Most people have no idea how big or powerful this industry has gotten. While some argue that data collection makes our online experience better through personalized ads, the data broker industry needs serious federal regulation because these companies collect our personal information without really asking us, use that information in ways that can hurt our economic opportunities, and operate with way too much secrecy for a democratic society.

The biggest problem with data brokers is that they collect huge amounts of personal information from places most people do not even know about, and they make profiles on us without getting real permission. According to a report by the Federal Trade Commission (2014), data brokers get their information from "public records, online shopping, loyalty cards at grocery stores, and social media." These companies combine all that information to create detailed profiles that might include someone's income, interests, shopping habits, or even health conditions. Shoshana Zuboff (2019) explains in her book *The Age of Surveillance Capitalism* that "even the small things we do online—like scrolling through a page or clicking a button—are tracked and used to make these profiles" (p. 134). This shows that consent is basically meaningless in the current system. While people might technically agree to terms of service, they have no real understanding of how much their data is being collected and shared with companies they have never heard of. The tracking happens automatically and invisibly. Scrolling and

clicking are not conscious decisions to share data, but they get treated that way. When companies collect information in ways we cannot see and make profiles without clearly asking us, they are violating our basic privacy rights, and that is a problem that needs regulation to fix.

This is not just about the idea of privacy—data brokers actually cause real problems in people's everyday lives by helping companies discriminate in pricing, lending, and other important decisions. In an NPR interview, Robert Siegel points out that "with each interaction we have online, companies collect data about us—what car we own, how big our mortgage is. Companies keep files on us, and they use those files to decide what to sell us and at what price" (Angwin, 2016). Julia Angwin adds a troubling example: "every website you visit creates itself the moment you arrive... we have found that there are cases where companies determine the price of the product to you based on where you live" (Angwin, 2016). These are not just things that might happen—these are documented cases where data broker information led to discriminatory pricing. This finding is supported by research from the Electronic Privacy Information Center, which shows how data profiles can lead to unfair outcomes in housing, employment, and credit decisions ("EPIC - Data Brokers," n.d.). When someone pays more for a product or gets rejected for a loan because of data they did not even know existed and cannot fight back against, that is just not fair. These practices can make existing inequalities worse and create new types of discrimination based on what algorithms think about our data.

Perhaps the scariest thing is that data brokers make it possible for political campaigns to manipulate voters with incredible precision. According to an investigation by *The New York Times*, "political groups use this data to send very specific messages to voters based on their personality, fears, or beliefs" (Thompson, 2020). Thompson calls this the "weaponization" of personal data—basically, information that was collected for selling stuff gets used to influence

how people vote. When political campaigns can use detailed profiles to exploit people's individual fears, democracy stops working the way it should. Voters are not all looking at the same information and making their own decisions. Instead, they are being individually targeted with messages designed to push their specific buttons. Using data broker information to manipulate voters is not just bad for individual privacy. It is a genuine threat to democracy, which makes regulation absolutely necessary.

Of course, not everyone agrees that data brokers are this problematic. People who defend data brokers argue that these companies provide valuable services for both regular people and businesses. They say data collection lets companies show us ads for stuff we actually want, and it makes online services work better—plus a lot of them are free because of advertising. It is true that personalized recommendations can be helpful, like when Netflix suggests shows you might like or when online stores show you products you are interested in. A lot of websites and apps we use every day are free specifically because ad money, powered by data collection, pays for them. However, this argument ignores the main problem: choice. The current system does not ask people if they want to make this trade. It just assumes we are okay with it through confusing terms of service and invisible tracking. Plus, the benefits—slightly better ads and free services—do not come close to matching the problems: discriminatory pricing, political manipulation, and complete loss of privacy. Regulation does not mean getting rid of all data collection. It means creating a system where people actually choose to participate, understand what they are giving up, and have real protection against misuse.

The way data brokers currently work—collecting information without real permission, enabling discrimination, and helping political manipulation—demands strong federal regulation to protect individual rights and democracy. As this essay has shown, data brokers operate

through invisible collection methods that make true consent impossible, their data gets used to make decisions that hurt people's economic opportunities, and their services allow the manipulation of democratic processes. While the industry says it provides valuable services, those benefits do not justify the current free-for-all with personal information. The push for regulation, like California's Consumer Privacy Act and advocacy from groups like the Electronic Frontier Foundation, shows that more people recognize that privacy is not just a personal preference—it is a basic right in our digital world. As Hayley Tsukayama (2025) warns, "without consequences to back up our rights... many companies will bank on not getting caught, or factor weak slaps on the wrist into the cost of doing business." People always say that data is the new oil, a valuable resource that powers the digital economy. But there is a huge difference: oil does not belong to anyone until it gets pulled out of the ground. Your data already belongs to you. The question is not whether data is valuable, it is who gets to decide how that value gets used, and whether you will have any say in it.

References

Angwin, J. (2016, October 19). ProPublica reveals discriminatory pricing by computer algorithms (R. Siegel, Interviewer) [Interview]. In *All things considered*. NPR. https://www.npr.org/2016/10/19/498582157/propublica-reveals-discriminatory-pricing-by-computer-algorithms

California Legislative Information. (2018). *California Consumer Privacy Act of 2018*. State of California. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Electronic Privacy Information Center. (n.d.). *EPIC - Data brokers*. https://www.epic.org/issues/consumer-privacy/data-brokers/

Federal Trade Commission. (2014, May). *Data brokers: A call for transparency and accountability*. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

Thompson, S. A. (2020, October 20). How political campaigns weaponize your data. *The New York Times*. https://www.nytimes.com/2020/10/20/technology/political-campaigns-data.html

Tsukayama, H. (2025, August 4). Data brokers are ignoring privacy law. We deserve better. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2025/08/data-brokers-are-ignoring-privacy-law-we-deserve-better

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

AI Disclosure: I used Claude to help me find sources and to check my APA formatting. I also asked it to explain some of the more complicated parts of the FTC report in simpler language. I did not use it to write any sections of my essay. The ideas and words in this paper are mine, and I can explain and defend every argument I make.