Duke SANFORD | CYBER POLICY PROGRAM

Response from Duke University's Data Brokerage Research Project

Consumer Financial Protection Bureau (CFPB) Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

July 2023

Introduction

The data brokerage research team at Duke University's Sanford School of Public Policy welcomes the opportunity to comment on the Consumer Financial Protection Bureau (CFPB)'s request for information regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information.[1] As the collection, analysis, monetization, and exploitation of people's information becomes more commonplace, regulatory attention to this issue is vital to protecting consumers and safeguarding the privacy, autonomy, financial security, and physical safety of all Americans.

We support the CFPB's continued attention to these important issues of data brokerage, the collection and sale of financial data about Americans, and harms to consumers and society.

About Our Program

The data brokerage research team at Duke University's Sanford School of Public Policy studies the data brokerage ecosystem—broadly, the collection, aggregation, analysis, buying, selling, and sharing of data. It studies the ecosystem's data collection and use practices, the controls that brokers do or do not place on their activities, and the risks that data brokerage poses to civil rights, consumer privacy, physical safety, and national security, as well as to specific populations like survivors of domestic and intimate partner violence, elderly Americans, and people with Alzheimer's. In line with the broader mission of the Sanford School of Public Policy, it focuses its work on affecting meaningful public policy change.

In accordance with an academic intellectual independence policy, all signatories on this document sign in their personal, not institutional, capacities. The comments submitted herein do not necessarily represent the views or positions of Duke University's Sanford School of Public Policy or Duke University.

Previous Policy and Legislative Engagements

For additional background and context, the team would direct the CFPB to previous Congressional and state-level testimony by our project lead, Justin Sherman,[2] previous Congressional testimony on data brokers by Professor David Hoffman,[3] and our team's response to the Federal Trade Commission (FTC)'s Rule on Commercial Surveillance and Data Security from October 2022.[4]

Question 1 asks, "What types of data do data brokers collect, aggregate, sell, resell, license, derive marketable insights from, or otherwise share?" We respond:

The data brokerage ecosystem gathers and sells data on virtually every American. Data brokers collect, aggregate, sell, resell, license, derive marketable insights from, or otherwise share data about individuals' demographics (including age, race, ethnicity, sex, gender, sexual orientation, religion, and marital status), political preferences and beliefs, home addresses, geolocations, health conditions (including diabetes, cancer, Alzheimer's, dementia, anxiety, and depression), financial well-being (including net worth, credit score, and debt estimates), and personality and lifestyle characteristics (such as travel, media consumption, and mobile app usage).[5] There are single US data brokers that collect and aggregate data on hundreds of millions of people in the United States. There are also US data brokers that additionally collect data on millions of people living in other countries. A single data broker might have anything from a few data points about a particular individual to hundreds or thousands of data points about a single person.

Data brokers frequently aggregate this data with the intent of packaging it, focused on particular subsections of the population. For example, in 2013, the Senate Commerce Committee published an investigative report that described data broker marketing packages on financially vulnerable consumers. The dataset titles included "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Retiring on Empty: Singles," "Tough Start: Young Single Parents," and "Credit Crunched: City Families."[6] In the FTC's 2014 report on data brokers, it highlighted such dataset titles as "Thrifty Elders" (late-60s and early-70s singles in "one of the lowest income clusters"), "Rural Everlasting" (single people over 66 with "low educational attainment and low net worths"), "Metro Parents" (people "handling single parenthood and the stresses of urban life on a small budget"), and other datasets targeting marginalized or vulnerable individuals with low incomes.[7] Some data brokers, the FTC said, even offered an "Assimilation Code," denoting, as the FTC described it, "a consumer's degree of assimilation to the English language."[8] Much of this is sensitive and pertains to protected classes of individuals as well as attributes that can be used for discrimination.

The list goes on. In August, Alfred Ng at *Politico* found 30 different data broker listings of data on pregnant people—or listings for companies to run advertisements to those people.[9] Just days earlier, Shoshana Wodinsky and Kyle Barr at *Gizmodo* uncovered 32 different data brokers advertising information on millions of pregnant and potentially pregnant people, sold on a cost-per-mille (cost per thousand ads) basis, meaning, as the journalists wrote, "that whoever buys them only pays for the number of end-users that are reached with a given ad."[10] Joseph Cox at *Motherboard* has written numerous stories about data brokers that gather individuals' phone location data, package it, and sell it to clients on the open market.[11] Privacy expert Pam Dixon's 2013 Congressional testimony highlighted data brokers advertising data on people with HIV/AIDS, people undergoing cancer treatment, people taking medications for Alzheimer's and blood disorders, and "rape sufferers," among others.[12] Dixon also highlighted brokers advertising lists of domestic violence shelters, a list of police officers at their home addresses, a list of people affected by drug and alcohol addictions, and a list of seniors currently suffering from dementia.[13]

Our research at Duke University has identified and analyzed data brokers selling datasets focused on elderly Americans, people suffering from Alzheimer's and dementia, students, employees, first responders, medical professionals, current U.S. federal government employees, and current and former members of the U.S. military, among many others.[14] Our project lead has also seen datasets for sale about people suffering from cancer, gambling addicts, families in debt, members of the LGBTQ+ community, environmental activists, supporters of Black Lives Matter, children, teenagers, and much more.

Question 1(a) asks, "What do data brokers do with the data they collect other than the aggregation, selling, reselling, or licensing of data?" We respond:

Many data brokers will provide buyers with datasets upon transfer of funds. Additionally, data brokers might offer identity verification services, such as transcript verification for students or income verification for prospective employers and landlords. In these situations, data brokers may not provide the buyer with access to the entire dataset but will instead permit the buyer (whether a large company or a landlord) to query the database against the information they have on file. For instance, a landlord could input information about a prospective tenant into the data broker's system, and the system would tell the landlord whether the information submitted matches the data on file about the prospective tenant. Examples of these kinds of datasets include Equifax's The Work Number, which contains employment and salary data on hundreds of millions of Americans,[15] and LexisNexis' public records search guide.[16]

There are also data brokers that have permitted their customers to run targeted advertisements to individuals on whom the broker has collected data. For example, in 2015, a Massachusetts-based data broker tracked people visiting reproductive health clinics in multiple other states through their phone geolocations and then sold targeted ad access to those devices to anti-abortion groups; they then ran manipulative, anti-abortion ads to people sitting in clinic waiting rooms.[17] (The Massachusetts Attorney General reached a settlement with the company and its owner in 2017 to ensure the company would not use the geofencing technologies near Massachusetts healthcare facilities, which the Attorney General argued would violate state consumer protection law.)

Finally, many data brokers use the data they initially gather to derive additional data about individuals. This "inference" could range from simpler techniques, such as using the mere fact that someone downloaded a religious app or LGBTQ+ dating app to infer sensitive data points such as religion and sexual orientation; to more sophisticated techniques, such as following individuals' smartphone geolocation patterns over time to learn about their visits to home, work, retail stores, medical facilities, gay bars, and places of worship. Brokers can then sell and license the inferences as part of their datasets, as well as integrate the inferences into their other services.

Question 1(b) states, "Please provide information about specific types of data that are financial in nature, such as information about salary, income sources, spending, investments, assets, use of financial products or services, investments, signals of financial distress, etc." We respond:

Our team has purchased data directly from data brokers about members of the U.S. military, with our findings to be detailed in a forthcoming report (based on a 2022-2023 study period). Within the datasets provided by brokers, we found several fields related to finances, including estimated income, estimated net worth, estimated home value, estimated credit rating, and presence of foreign investments, to name a few. We did not attempt to validate this data, and we do not know the accuracy of this data. Furthermore, the U.S.' three major credit reporting agencies, which fall under our definition of data brokers—Equifax, Experian, and TransUnion—gather and sell data well beyond the scope of statutorily covered credit reporting data, alongside that brokerage of credit information.[18]

Question 2 asks, "What sources do data brokers rely on to collect information? What collection methods do data brokers use to source information?" We respond:

Data brokers gather data about people in three main ways:[19]

1. *Directly*, including data brokers buying up companies and services that gather data directly (such as apps and websites) and paying app developers to use the data broker's software development kit (SDK) in the developer's app, after which the developer can just let the app run while the broker "sits" within the app and siphons data on users;
2. *Indirectly*, including data brokers scraping public records (e.g., property records, voting records, etc.), gathering data from real-time bidding networks for online ads, and paying app developers to transmit data to data brokers via server-to-server transfers, once the app developers have collected information on app users and stored it on their own servers; and
3. *"Inference,"* or prediction—data brokers using algorithms and other techniques to make predictions about individuals' characteristics, such as by using purchase information and home ZIP code to predict household income, location data from smartphones to predict religion (e.g., visits to churches, mosques, synagogues), or app installations on a phone to predict sexual orientation (e.g., the presence of LGBTQ+ dating apps).

These sources span apps, websites, advertising networks, and companies in a wide variety of industries, from retail and finance to transportation, entertainment, and technology.

Question 2(a) asks, "What specific types of information do data brokers obtain from public records databases? Which public records sources do data brokers use?" We respond:

Data brokers gather information from court records, motor vehicle records, property filings, voter registries, Census data, birth certificates, marriage licenses, divorce records, bankruptcy records, and by scraping public websites, among others.[20] Government records laws make this information public but entirely failed to—and still fail to—account for how the internet and the data brokerage industry make this information readily available for purchase and exploitation.

The U.S.' few state consumer privacy laws have virtually identical, complete carveouts for "publicly available information," which is explicitly defined to include government records.[21] As a result, "people search" data brokers scraping public records, aggregating them, and making them available for search and sale online are usually exempt from coverage under these state privacy laws. Consumers in California, for example, cannot fully exercise their opt-out rights for "people search" data brokers that scrape government records and then build and sell profiles of the individuals in them.

Question 2(b) asks, "Are people unknowingly deceived or manipulated into supplying data to data brokers? Describe the nature of such deception or manipulation." We respond:

Consumer consent is not an effective**,** administrable, or viable approach to the regulation of commercial surveillance. The current U.S. legal and private-sector approach results in a system in which individuals are effectively forced into having their data gathered and then quietly sold.

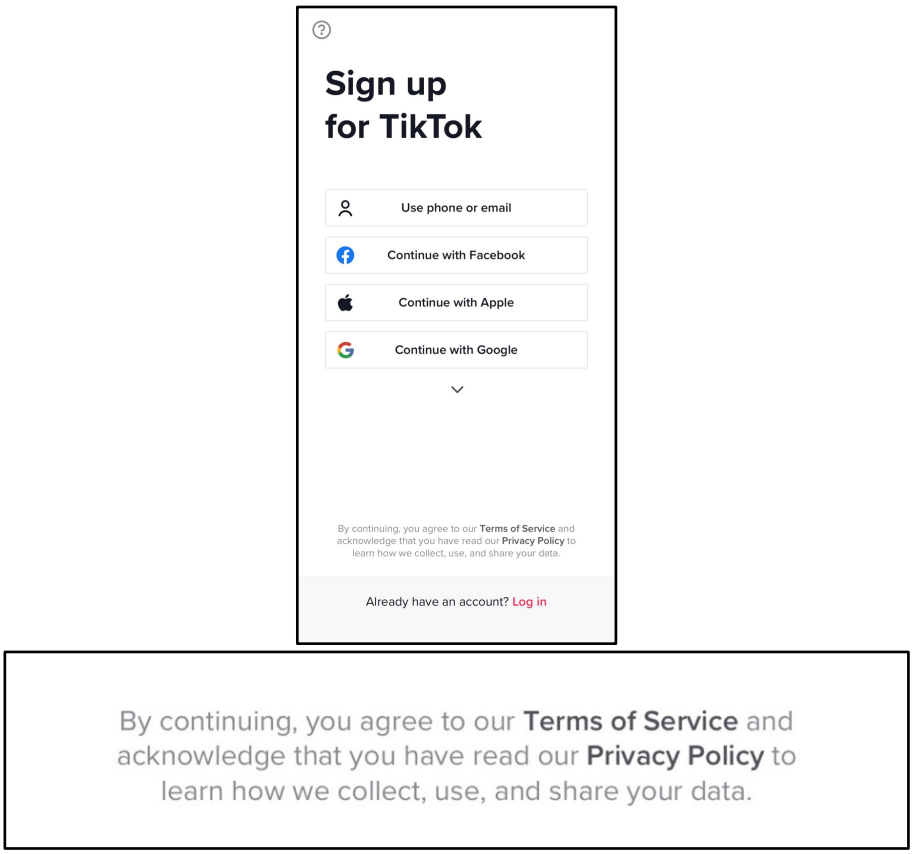
Companies often define consumer consent—and many laws and bills around the country define consumer consent—as a person simply using an application or service that has a privacy policy. That, however, does not accurately capture whether or not consumers fully know and understand the extent to which their data is going to be collected, used, and possibly sold or shared in the data brokerage ecosystem. Focusing on the individual also ignores the systemic problem at play; it is impossible for consumers to exist in American society without interacting with the data brokerage ecosystem in some form. Making the entire conversation about "consent," and a misleading idea of "consent" at that, avoids addressing the systemic collection, buying, selling, and sharing of consumers' data. A system in which data collection is the default and opting out of data collection is a separate effort puts the burden on consumers to protect themselves against abusive data collection and use practices. Studies, some of which are discussed in the next paragraph, show that consumers

do not have the knowledge, understanding, or time to shoulder this burden of self-protection.

Using an app or service that also has a privacy policy somewhere—in a settings menu, in the footer of a website—is not a determinant of "consent." Most consumers do not even read privacy policies, and many studies have demonstrated this fact: a 2019 Pew Research Center survey found that 81% of Americans agree to privacy policies at least monthly, but that only 9% of Americans say they always read a privacy policy before agreeing to a company's terms and conditions.[22] A 2021 survey by Security.org found that 37% of people skim the documents, 35% don't read them at all, and 16% search for and read a few key parts of the documents;[23] only 11% say they fully read privacy policies before agreeing.[24]

The information asymmetry facing consumers is also huge: a 2008 study calculated that if consumers wanted to read the privacy policies for the services they use, it would take each person an average of 244 hours a year.[25] As the authors put it, "the national opportunity cost for just the time to read policies is on the order of $781 billion."[26] The *New York Times*, to give another example, did an investigation into 150 companies' privacy policies in 2019 and found that they were difficult to read (an "incomprehensible disaster," is how the title of the article put it"), with many even more complex than the texts that doctors, lawyers, and other professionals must understand in their jobs.[27]

Ironically, companies have the ability to track whether consumers are actually reading their privacy policies—they could, and many already do, monitor for how long a person views a webpage and whether they view all the content—but they choose to take a consumer not reading or understanding a document, and using an app or service anyway, as permission to gather and use their data. For example, TikTok has a common disclaimer at the bottom of the app, upon download, that mirrors the claims of many other companies providing digital apps and services: "By continuing, you agree to our Terms of Service and acknowledge that you have read our Privacy Policy to learn how we collect, use, and share your data."



This is not consent.

Even apart from the issue of not reading privacy policies, most consumers do not reasonably understand how the data brokerage ecosystem operates. Although public understanding around data collection is growing, that does not include awareness of the ways that companies gather information on consumers through websites, mobile applications, and other products and services, and then sell and share the data with other actors. An individual downloading a weather app with a built-in GPS feature has no reasonable expectation the app might share their location data with a data broker who then sells it to advertisers and federal law enforcement. (The FTC took an enforcement action in this vein in 2013 against flashlight app Brightest Flashlight Free, which indicated to users that location data would only be used internally but in reality shared and sold the data with third parties.[28]) At times, privacy policies are outright deceptive, such as Flo Health who stated that an individual's sensitive data would not be shared with third parties, only to sell that data to Google, Facebook, and Flurry.[29] Moreover, even if consumers did understand how the data brokerage ecosystem operates, that is distinct from fully understanding its harms. And even if consumers did fully understand what was happening, the focus on individuals distracts from the systemic problems at play—and the immense amount of information and financial asymmetries stacked against consumers. People are regularly forced to interact with data

brokers, whether to get a new credit card, put in a deposit for an apartment, or apply for a loan; whether or not they "consent" is not a question limited to merely using an app that has a privacy policy somewhere if their not-consenting means they cannot access housing, money, employment opportunities, and other essentials.

Question 2(c) asks, "What technological components facilitate brokers' collection of data, including but not limited to: tracking scripts, web-based plug-ins, pixels, or software development kits (SDKs) in Apps?" We respond:

Data brokers use different technological mechanisms to collect data, including but not limited to:

1. *Software Development Kits*, used to build apps, are currently subject to some rules by the Apple App Store and Google Play Store. However, these restrictions typically cover location data, not other forms of data sharing and profiling, and are poorly enforced, leading to continued violations.[30] Ultimately, SDKs remain a viable way for data brokers to collect data.
2. *Pixels*, which are typically embedded in websites and emails, collect information about consumer interactions, clicks, and even information entered into forms. These packets of code have recently come under scrutiny from the FTC, as they enabled health data breaches via the collection of sensitive health information on hospital websites and other digital health platforms.[31] The FTC identifies a few major consumer rights concerns with pixels, including the lack of transparency around pixel use; the ability of companies to connect information collected by pixels (including financial information) to purchases, social media accounts, and more; and a failure to appropriately remove personal information or "de-identify" protected data.[32]
3. *Tracking Scripts* are a more sophisticated version of tracking pixels that present many of the same issues and collect much of the same information. Of note, numerous Congressional websites have utilized tracking scripts that share visitor information with data brokers and advertisers.[33]
4. *Server-to-Server Transfers* allow app developers to directly collect location or personal information on users, then transfer it directly to data brokers.[34] This process largely occurs out of sight, with next to no visibility into the types of user data collected or the parties that receive it. These transfers have therefore emerged as a way for data brokers to get around app store-imposed requirements limiting the inclusion of some types of SDKs in apps.
5. *Data Scraping*, which has been the focus of recent attention at Twitter, Reddit, and other social networks, often occurs through bots or API plug-ins that collect high volumes of user data from social media, websites, or the internet at large.[35] These kinds of scraping tools can also be used to gather information from public records,

which are then aggregated, tied to individuals, and posted online for sale by "people search" data brokers.

These are a few of the most notable ways that data brokers collect data directly from website or app user behavior. But, as addressed below, a variety of partnerships and contractual relationships also help provide data to data brokers.

Question 3 asks, "What specific types of information do data brokers receive from financial institutions? Do financial institutions place any restrictions on the use of this data? Under what circumstances do consumers consent to this data sharing or receive an opportunity to opt-out of this sharing?" We respond:

It is difficult to say precisely what type of data is sold to data brokers by financial institutions. We know that many data brokers sell prebuilt marketing or mailing lists as standalone products, drawn from financial data the brokers gather as well as information the brokers infer about consumers.[36] Financial institutions also offer data "augmentation" services, where a broker provides data it already possesses on individuals to a financial institution, which in turn uses its collected data to update inaccurate records or generate additional insights. Some of these insights include purchasing behavior and preapproval for certain types of services, among others.[37]

Consumers in some states are legally given the ability to opt-out of the disclosure of their information to third parties, except when legally required or when subject to an exemption (such as for "publicly available information"). Opt-out mechanisms typically require a user to individually visit each financial institutions' webpage and submit an online request. These are imperfect solutions. Many consumers are unaware that an institution even has their personal data. Consumers also need to interact with the credit and loan industries to function in the United States, yet in doing so they are often forced to interact with or have their data gathered and sold or otherwise used by data brokers.

Question 4 asks, "What specific entities and types of entities have relationships (e.g., partnerships, vendor relationships, investor relationships, joint ventures, retail arrangements, data share agreements, third-party pixel usage) with data brokers? Describe the nature of those relationships and any relevant financial arrangements pursuant to such relationships." We respond:

Business relationships between mobile applications and data brokers are extremely common. Often, data brokers provide app developers with an SDK, for use in developing their mobile apps, that feeds data back to the data broker.[38] This could range from location data to app download and usage information. App developers are incentivized to include these

SDKs in their apps because data brokers pay them to do it; the location data broker X-Mode, for instance, was paying some app developers $10,000 or more a month for access to their users' smartphone locations.[39] In order to avoid detection via Apple and Google's growing SDK transparency efforts, data brokers also pay app developers to conduct server-to-server transfers of user data.

Data brokers may have partnerships with one another, from data-sharing arrangements to integrated service offerings. Numerous data brokers also have relationships with data broker "clearinghouses" that act as centralized, online marketplaces where prospective data buyers can find data about people, devices, and places from a variety of broker sources. Some of these clearinghouses provide buyers with discounts if they purchase data through the clearinghouse as opposed to directly from a broker, suggesting a spectrum of financial relationships between clearinghouses and data brokers.

The majority of educational institutions have partnerships with the data broker National Student Clearinghouse to process student data. A public records request to New York and Los Angeles Public School Districts found that these public schools shared student directory information with the data broker National Student Clearinghouse, as well as with military recruiters, and community colleges.[40] Many post-secondary schools report data to the National Student Clearinghouse's Student Tracker (which covers 97% of all students) to document student and degree data.[41] National Student Clearinghouse does not need to attain students' consent before acquiring their data because FERPA § 99.31 permits the disclosure of education records to authorized third parties.[42] National Student Clearinghouse shares "postsecondary enrollment status and institution name for the previous six months" with Equifax for pre-employment verification services.[43] The Work Number, Equifax's employment verification service, markets that "only Equifax can provide instant education verification through the National Student Clearinghouse using only the loan applicant's Social Security number."[44] In 2021, Equifax announced its "exclusive integration" with the National Student Clearinghouse for pre-employment verification offerings. Potential employers or banks verifying loans can access these reports through Equifax. Student data can influence the financial position of a student or recent graduate seeking a loan or employment. National Student Clearinghouse receives student data from schools as an authorized third party and Equifax receives student data from National Student Clearinghouse through their exclusive integration.

Question 5 asks, "Which specific entities and types of entities collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties?" We respond:

Many websites, mobile apps, retail stores, online marketplaces, connected device companies, data brokers themselves, and other companies as well as online products and services are all involved in the collection and then selling, licensing, or sharing of consumers' data.

The main source of brokered data may also vary depending on the type of data in question. For instance, many data brokers selling geolocation data get the data from mobile apps on people's smartphones. In the health space, a range of websites, apps, companies, data brokers, advertising firms, social media networks, and others outside the scope of the Health Insurance Portability and Accountability Act (HIPAA) can and do legally collect, share, and sell Americans' identifiable health data with third parties.

Question 6 asks, "Does the granular nature of data brokers' collection of information related to consumer preferences and behaviors influence consumer purchasing patterns or levels of indebtedness? Describe the nature of such collection and how it may influence purchasing patterns." We respond:

Manipulative designs intended to deceive or influence customers, known broadly as "dark patterns," have come to the attention of both the public and regulators in the past few years before 2020. The FTC published a report earlier this year detailing serious concerns with the use of manipulative designs, often informed by detailed consumer data and profiling, to influence consumer purchasing and behavior and encourage users to opt in to intrusive data sharing practices.[45] This report was followed closely by an enforcement action against Amazon, which the FTC alleges used some of these practices to trick customers into subscribing to Amazon Prime then making it incredibly challenging to unsubscribe.[46]

The use of customer profiles and high-volume data analytics to influence purchasing behavior is well-documented, and as the FTC begins leveraging enforcement actions against companies for the abuse of "dark patterns," the extent of use cases will likely become clearer. Data brokers contribute to this ecosystem by selling to their buyers a wide range of data, including sensitive and individually identified data, about consumers' demographics, habits, lifestyles, personal preferences, health conditions, and much more. Such data can be used in combination with technical designs, algorithms, advertising technologies, and other mechanisms to influence consumers.

Question 7 asks, "How do companies collect consumer data to create, build, or refine proprietary algorithms?" We respond:

Artificial intelligence (AI) systems typically rely on large datasets to train models and produce outputs. In addition to collecting data from their users, scraping websites, or partnering with other businesses (among others), companies could get this data to train AI systems by purchasing it from data brokers. The data brokerage ecosystem gathers and sells data about hundreds of millions of Americans, as well as devices and locations, which companies might want to use in building AI systems. Given the fact that much of this data is gathered and sold about Americans without their fully informed and expressed "consent," this creates additional privacy risks to individuals.

It is also worth noting that many data brokers use algorithms internally, leveraging the very data that they gather and sell. For example, one of the data brokers caught selling data about elderly Americans and people with Alzheimer's to criminals had internal algorithms applied to the data; when someone was victimized by a scam, the system would mark those people as responsive to that kind of advertisement or mailer (a scam), resulting in a cycle of revictimization.[47]

Crucially, data brokers also fit into at least three buckets of concerns about AI broadly: the scraping and harvesting of sensitive information and intellectual property to train systems (which can come from data brokers); the quality, representativeness, and accuracy of the data used to train AI systems (when that information comes from brokers, whose data quality and accuracy varies); and the lack of transparency into AI development and decision-making (which can be exacerbated when the data used to train a system comes from the opaque data brokerage industry).

Question 9 asks, "Can people avoid having their data collected?" We respond:

Consumers in the U.S. cannot reasonably avoid having their data collected and sold by data brokers. There are some existing, relatively narrow federal laws and regulations that place controls around the collection, use, and sharing of certain types of data by certain types of covered entities. But data brokerage is mostly unregulated, and these existing, relatively narrow laws focus just on how some entities in a few select industries or sectors use specific kinds of data. It is also worth noting that many data brokers do not have a direct relationship with the individual and gather data from public records and from entities that do not clearly and fully disclose they are transferring data to the broker.

For example, the Health Insurance Portability and Accountability Act applies only to certain covered health entities, like hospitals and primary healthcare providers, and does not apply

to mobile health apps, social media companies, online advertisers, data brokers, and many other kinds of corporate actors. These organizations outside the narrow scope of HIPAA are therefore free to legally gather, buy, package, sell, and share people's health-related data—and they do, such as whether people have prescriptions for antidepressants or whether they are believed to be pregnant. The Family Educational Rights and Privacy Act (FERPA) is another example. FERPA governs covered educational institutions' use and disclosure of students' data—but its narrow scope allows many other actors, including those brokering data, to sell information about students with virtually no restrictions.

Data brokers also have a wide and deep reach in the United States. Many consumers cannot realistically apply for a job, loan, or housing or interact with a private insurance carrier without—knowingly or not—interacting with a data broker or having their data trafficked by a data broker in some form.

Question 9(a) asks, "Are there certain special populations that are less likely to be able to exercise control over the collection, aggregation, sale, resale, licensing, or other sharing of their data?" Question 9(b) asks, "If so, which special populations, and why?" We respond:

Even if Americans did have comprehensive rights to exercise control over the brokerage of their data, individuals would require the time, resources, and knowledge to do so. Poorer Americans, people for whom English is a second language, individuals with visual impairments, elderly people, and others may be even more disadvantaged when it comes to exercising rights that could hypothetically be provided. Further, whether consumers know it or not, it is incredibly difficult if not impossible in the U.S. to apply for a loan, a job, or housing or have private insurance without interacting with a data broker in some form. They are ingrained into those vital functions of accessing finances, employment, a place to live, and health and other kinds of coverage. Individuals battling further systemic inequities within those systems, such as Black and brown people interacting with the U.S. health insurance and housing systems, have even less ability to escape the reaches of the data brokerage ecosystem and may be even further pressured to provide more of their data to brokers.

Children and teenagers cannot be expected to understand privacy policies and terms of service—especially as previously mentioned studies show adults do not understand them—and meaningfully exercise the limited control options they might have over some of their data. This is particularly true for any children or teenagers in some of the communities mentioned above, such as people for whom English is a second language. In the educational context, students are often not notified by schools when their information is shared with data brokers, and the process for opting out is not well documented.[48] Students from ages

13 to 17 have no way to consent to the publication of their personal information because they are below the age of an "eligible student" which can opt out under the Family Educational Rights and Privacy Act (FERPA).[49] COPPA imposes restrictions on collecting data about children under the age of 13, but it only regulates companies and does not apply to schools.[50] A parent could also consent to share the student's data.[51] Even if students can opt out of having their directory information reported, many schools make this process challenging. The WPF report identifies that only "39 percent of studied primary and secondary schools make FERPA opt out forms online and available to the public."[52] Data brokers also sell data about children and even more so about teenagers aged 13 to 17 years old. For example, data broker Exact Data was willing to sell lists of "fourteen and fifteen year old girls for family planning services" to buyers.[53]

It can be harder for elderly Americans and people with Alzheimer's to exercise control over their personal data for institutional and generational reasons. Several data brokers have been prosecuted by the Department of Justice for intentionally targeting "elderly and vulnerable Americans" by repeatedly selling their personal information to criminal scammers.[54] The data brokers created lists of elderly and vulnerable Americans who were already scammed once and resold those lists to scammers.[55] Since data brokers have repeatedly profiled elderly individuals with cognitive impairments to help scammers take advantage of them, the institutional practices of the data brokerage industry can put elderly Americans at risk of harm. Many elderly Americans have also not received the digital education that younger generations have, do not have the same levels of digital literacy, and are perhaps even less likely to understand the full implications of agreeing to a privacy policy or registering for an unverified mailing list. Extra protection measures should be adopted to protect elderly individuals and people suffering from brain health issues from deceptive targeting.

Question 10 asks, "Under what circumstances is deidentified, 'anonymized,' or aggregated data reidentified or disaggregated?" We respond:

There are important computer science and statistical techniques that provide enhanced protection of individuals' data in datasets, such as differentially private algorithms. However, there are also cases in which data brokers claim data is "anonymized" or "deidentified" when that is not the case.[56] In this way, "anonymization" is often a marketing term used by data brokers to falsely suggest that it is impossible to link a dataset back to individuals. The reality is that it is all too easy to run analytics on datasets or combine datasets together in order to identify the specific people within them.[57] Further, many data brokers base their business model on being able to identify individuals for their customers, whether those customers be law enforcement agencies, marketing firms, or criminals. For instance, the data broker Fog Data Science advertised to law enforcement customers that its location data was

"anonymized" and simultaneously advertised features to "deanonymize data by revealing device advertising IDs, IP addresses, and other phone details."[58]

Over the years, researchers and journalists have linked supposedly "anonymized" data on AOL web searches, Netflix user movie ratings, and New York City data on taxi rides back to specific people.[59] One recent study found that with only 15 specific demographic attributes, it would be possible to "re-identify" 99.98% of Americans in a dataset.[60] The FTC's 2022 lawsuit against data broker Kochava stated that "the location data provided by Kochava is not anonymized" because "it is possible to use the geolocation data, combined with the mobile device's [mobile advertising ID (MAID)], to identify the mobile device's user or owner."[61] There are many other examples and studies demonstrating this point. Data brokers' and other companies' use of persistent identifiers like mobile advertising IDs makes it even easier to track specific people across datasets and to identify them by combining datasets.

These technological capabilities for data aggregation, individual identification, and consumer tracking are fast-evolving, but U.S. law and policy moves much more slowly. Legal and regulatory discussions about what is considered "identifiable" or "personally identifiable information" often focus on the most well-known identifiers such as name and Social Security Number. These discussions reflect outdated views of the technological capabilities that exist today and the new identifiers, such as unique device identifiers and mobile ad IDs, that can be used to identify individuals and track them across devices and datasets. Using legal definitions of "reidentification" or "deidentification" as they exist today may limit policymakers' and regulators' ability to fully assess and appreciate the risks and potential harms to individuals.

Question 11 asks, "Can people reasonably avoid adverse consequences resulting from data collection across different contexts (e.g., cross-device tracking, re-identification, mobile fingerprint matching)?" We respond:

People cannot reasonably avoid the adverse consequences resulting from data collection across different contexts. Organizations have a continually greater ability to combine datasets to learn more information and identify individuals, "reidentify" individuals in datasets whose identities have been masked, and track individuals across environments through the use of unique identifiers, mobile advertising IDs, and other linked data points. Data brokers specialize in these kinds of activities. Many data broker clients pay for this very kind of cross-context tracking of consumers.

Many data brokers also sell information to each other, making it even harder for consumers to avoid certain harmful aspects of the data brokerage industry.[62] For example, Acxiom has

partnerships with other data brokers, including Corecom and Nielsen.[63] In the FTC's 2014 report on data brokers, it found that seven out of the nine studied data brokers were selling data to each other.[64] Data brokers often do not inform the consumer when they share information on them, as with LexisNexis preventing business partners from referencing its products in third-party disclosures.[65] This lack of transparency makes it more difficult for consumers to know which data brokers have their personal information.

Question 12 asks, "Which specific entities and types of entities purchase data from data brokers? How do these entities use the purchased data?" We respond:

The range of entities who purchase data from data brokers vary widely, as do their uses of the purchased data. Many entities purchase data from brokers for marketing purposes, from mail campaigns to tailored online marketing. Entities also purchase data from data brokers for uses such as fraud detection, identity verification, or market research.[66] However, nefarious individuals have previously purchased data that is then used to commit acts of violence or abuse.[67] Law enforcement agencies are known to purchase data from location-based and many other kinds of data brokers, often without a warrant.[68]

Question 12(a) asks, "What specific uses concern marketing, decisioning, fraud detection, or servicing related to consumer financial products and services?" We respond:

Data brokers sell prepackaged datasets that can be used for direct mail, email, phone, or internet-based marketing. These datasets are often titled with a given characteristic, such as the aforementioned "Credit Crunched: City Families."[69] Many brokers allow purchasers to create custom-made lists broken down by any of the data points they gather about individuals, such as geographic location, age, income, political affiliation, or interest in a certain hobby.[70] Location-based brokers can provide insights about mobile devices that enter a certain area or generate inferences based on a given individual's movements. Some brokers, especially credit reporting agencies, offer data "augmentation" services that correct inaccuracies in a dataset provided by the purchaser.[71] Others offer fraud detection and identity verification services to their customers.[72]

Question 12(b) asks, "What, if any, restrictions do data brokers impose on the use of such data?" We respond:

In our team's research, during which we have purchased data from data brokers (through university research ethics processes), we have found that data brokers often restrict the sharing or reselling the data they broker.[73] Beyond that, however, we have found that brokers impose very few restrictions on the actual use of data, such as what kind of analysis

can be done on the data, how individuals encompassed in the datasets could be targeted (beyond standard disclaimers to not violate the law, such as with scams), and on whether and how buyers can combine the purchased data with other data to identify individuals or build bigger profiles of them.[74] On top of this, some data brokers require prospective buyers to sign a nondisclosure agreement (NDA) before purchasing data or, sometimes, before even speaking with a sales representative.[75] Many data brokers do not make any attempt at verifying their customers' identities, and we have purchased individually identified, sensitive, non-public data about individuals from data brokers with no vetting—or where we were even given an option to skip the vetting process.

Question 13 asks, "What data broker practices cause harms to people? What are those harms and types of harms?" We respond:

The data brokerage ecosystem threatens Americans' freedoms and civil rights, invades their privacy, and poses risks to their physical safety. It also creates risks to U.S. national security. Our team's previous work has focused on areas such as data brokerage and scams, data brokerage and domestic violence, data brokerage-linked policing and state surveillance, and data brokerage and risks to military servicemembers.[76] Here, we focus our discussion predominantly on harms associated with credit reporting and consumers' financial opportunities and wellbeing.

Data brokers inaccurately reporting credit information causes financial harm to the person whose information is incorrect. Decisions about housing, credit, employment, and even access to vaccines depend on information provided by data brokers.[77] A 2022 paper from Northeastern University researchers, for example, found that Experian's coverage of adults in North Carolina is not only inaccurate, but performs worse for individuals from historically disadvantaged groups.[78] The research indicated that younger populations and ethnic minorities were more likely to have incorrect information in their credit reports than white individuals or those living in wealthier locations.[79] This inaccurate information can exacerbate economic inequality and unfairly restrict access to financial opportunities.

Students who have student loans can be harmed by the inaccurate reporting of student data. In 2020, students filed a class action lawsuit against credit reporting data brokers Great Lakes Educational Loan Services, Equifax Information Services, TransUnion, Experian Information Solutions, and VantageScore Solutions.[80] The student plaintiffs sued because these data brokers inaccurately reported data about student loan repayments which were suspended under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). The CARES Act became a law on March 27, 2020, and it provided economic relief to workers, students, families, and businesses.[81] In particular, it provided relief for student loan

borrowers by suspending all requirements for paying student loans owned by the U.S. Department of Education from March 13, 2020 to as long as 60 days after June 30, 2023.[82]

When many students stopped paying their loans at the beginning of COVID, data brokers reported that their payments were late.[83] This inaccuracy placed many students in increased financial distress during COVID. The misreported information caused the students to "suffer long lasting credit stigma, including inaccurate and lower credit scores resulting in no, limited or more costly access to credit."[84] The credit reporting data brokers worsened the situation by mishandling "desperately-needed federal relief granted to students under the Coronavirus Aid, Relief, and Economic Security Act.[85] The plaintiffs claimed that there was widespread misreporting of student loan data, as the "Defendants inaccurately reported the status and financial import of millions of borrowers' student loans."[86] According to the plaintiffs, data brokers inaccurately reported student data, causing immediate financial repercussions and long-term financial challenges for millions of students.[87]

Question 13(a) asks, "Are there certain special populations that are more likely to experience harms? If so, which special populations and why?" We respond:

Data brokers gather and sell data on hundreds of millions of Americans, of every race and religion, gender and sexual orientation, age, religion, income bracket, state and city, and political affiliation. The data brokerage ecosystem impacts virtually every single person in the country whether they recognize it or not—even children and teenagers under the age of 18, about whom numerous brokers collect and sell data.

Simultaneously, the harms of the data brokerage ecosystem, as with the harms of surveillance writ large, fall hardest on already oppressed or otherwise marginalized individuals and groups. These include, among many others, Black and brown communities that face disproportionate levels of policing;[88] poor families that already face barriers in accessing public services, medical care, housing, and employment opportunities;[89] elderly Americans, people with Alzheimer's and dementia, and others whom criminals could target because of their diminished cognitive capacity or susceptibility to scams;[90] people who are pregnant or could become pregnant and face increased levels of surveillance and criminalization concerning their health and body;[91] individuals suffering from depression and anxiety afflicted by stigma and barriers to care;[92] members of the LGBTQ+ community who face increased criminalization, discrimination, and threats of violence;[93] religious minorities and other faith communities targeted with hateful rhetoric and at risk of potential attacks on places of worship;[94] and children and teenagers who do not have the ability to meaningfully understand how data brokers monitor them and their families.[95] In each of these cases, data brokers gather and sell data about individuals that can exacerbate harms to individuals and groups, whether law enforcement purchasing data from data brokers

without warrants or anti-abortion or anti-gay organizations purchasing data to track and target specific individuals.

Additionally, there are national security risks associated with the availability of sensitive, identifiable data about active-duty U.S. military servicemembers and federal government employees. It is possible that a foreign government could exploit the fact that data brokers collect and aggregate this data at scale, and then package it, to profile and target individuals working in U.S. policymaking and the U.S. national security apparatus.[96]

Question 13(b) asks, "Are data brokers selling, reselling, or licensing information about particular groups, including certain protected classes? If so, what are examples of this behavior?" We respond:

Yes. Data brokers package and sell data that breaks down groups of individuals by such characteristics as race, ethnicity, sex, gender, sexual orientation, age, income, religion, children in the home, and more, many of which correspond to protected classes. When an individual or organization approaches a data broker to purchase data, they can request to buy this kind of data based on a pre-defined and pre-supplied list of data packages—or "marketing segments," in data broker parlance—that might be listed on the broker's website or in marketing materials.[97] Typically, data brokers also provide prospective buyers with a list of data points they have on file, which the prospective buyer can then use to request a specifically tailored dataset. For example, when former student researcher Joanne Kim contacted dozens of data brokers asking to buy data about Americans' mental health conditions, the conversations yielded discussions about how the data brokers might be able to tailor their datasets to her particular interests.[98] In this way, data brokers both sell data related to protected classes and permit their buyers to customize the finalized datasets that can contain protected class-related information.

Question 13(c) asks, "What harms do people experience if they are unable to remove their information from data broker repositories?" We respond:

By having their data available for purchase on the open market, individuals are constantly subject to the potential harms mentioned above. Additionally, by having their data stored in data broker repositories, individuals are at increased risk of their data being stolen by criminals and used maliciously, compounded by the fact that data brokers are prime targets given the immense amount of data they possess and the lax cybersecurity practices that many brokers follow.[99] There is also a risk that foreign states could exploit this aggregation of sensitive, non-public data to hack into data brokers and acquire information about certain targets, such as military servicemembers or government employees.

Question 14 asks, "What data broker practices provide benefits to people? What are those benefits?" We respond:

There are data brokers who offer services to verify individuals' identities, verify individuals' employment histories, verify individuals' college and university degrees, detect fraud, and conduct market research. Some of these practices, like fraud detection and degree verification, provide and have provided benefits to individuals and organizations. As mentioned in a newly published report from our team on the brokerage of student data, National Student Clearinghouse adds 5 million records annually to the Department of Education's student loan database and helps resolve 6.5 million errors in students' data every year.[100]

Question 15 asks, "What actions can people take to gain knowledge or control over data, or correct data that is collected, aggregated, sold, resold, licensed, or otherwise shared about them?" We respond:

Consumers may be able to request that some data brokers remove their information or stop selling their information in some cases, such as if the broker provides an opt-out request form under a state privacy law. On the whole, however, it is largely unavoidable that consumers will have their data collected and sold by data brokers, and opt-out requests are not a viable approach to the harms caused by the data brokerage ecosystem. In many cases, consumers likely do not know about data brokers or understand that they are obtaining their information (let alone how). New laws, regulations, and policies are needed—not placing the burden on individuals to fight systemic data brokerage surveillance practices.

Question 16 asks, "How can and does the activity of data brokers and their clients impact consumers beyond those whose data were collected or used by that data broker? How, if at all, can consumers reasonably avoid being targeted or influenced based on the activities of data brokers and their clients, even if they are able to avoid or opt-out of having their own data collected?" We respond:

Data brokers gather and sell data about virtually every American. When data brokers gather data about individuals, they may also gather or learn information about friends, family members, coworkers, and other people in those individuals' social networks. For example, if an adult's location data shows that they regularly drive up to a school during the week around 7:30am and 3:00pm, for just a few minutes each, that may strongly suggest that said person has a child at the school; even though the adult is the target of collection per se, the child is also impacted.

As described above, consumers cannot reasonably avoid being targeted or influenced based on the activities of data brokers and their clients. Even if they are able to avoid or opt-out of having their own data collected by certain brokers in certain cases, the data brokerage ecosystem is large, many consumers have never even heard of many of the thousands of data brokers in the U.S., and the legal and regulatory protections against data collection and sale from brokers are limited and confined to certain kinds of data gathered by certain entities. Data brokers have a considerable ability to gather data on virtually every American.

Question 17 asks, "What information do State-level data broker registries provide? How is this information made available and used? Are State-level data broker registries adequate to prevent harm? How could they be improved?" We respond:

There are two state laws, one in Vermont and one in California, that require certain companies that meet their definitions of a "data broker" to register with the state. Other states have considered these kinds of bills.[101] The information provided by these covered companies is then published online in a publicly viewable database.

Data brokers lobbied against these laws' passage, and the registries were an improvement over the status quo in the ways they made some more information about brokers more accessible to the public. However, these laws are fundamentally limited. They both define data brokers as only third parties, excluding the large number of "first-party" collector companies that gather information directly from consumers and then sell it (including to third-party data brokers).[102] For example, thousands of mobile apps sell data about their users to data brokers. Because they are selling data about individuals with whom they have—in the Vermont and California terminology—a "direct business relationship," they do not have to register under the law. Selling data on one's own customers should not be a reason to receive exemption from the registry.

Further, and more importantly, even with a few provisions around information security, these state registry laws do not place controls around data brokerage. They do not change how brokers collect, sell, and license information about people. They consequently fail to sufficiently protect Americans from the industry's harms. Many data brokers can and do file a registration with the state and largely continue with business as usual.

The penalty for non-registration is also small: in California, for example, just $100 per day.[103] In California this year, there are over 100 covered third-party data brokers that have failed to register with the state.[104] These include data brokers owned by TransUnion,[105] the large credit-reporting agency that can undoubtedly afford the small penalties for non-registration. Despite the existence of penalties, a few thousand dollars in fines a year does not sufficiently

incentivize a data broker to register, when it can make all that money back by selling a single dataset.

Our team has downloaded and analyzed these state registries as part of its research and found that there are multiple entries in each where the information is outdated or inaccurate, including incomplete fields, vague responses, and broken or inaccurate website links.[106]

Question 18 asks, "What controls do data brokers implement in order to protect people's data and safeguard the privacy and security of the public? Are these controls adequate?" Related, Question 9(a) asks, "What controls exist related to who can purchase or obtain information from data brokers?" And Question 9(b) asks, "Are these controls adequate?" We respond:

The extent to which data brokers place controls on the sale and use of their data is unclear and in need of further study. For example, our research has found that data brokers may have controls in some cases, such as internal requirements to vet clients before they sell or share information about consumers. Other brokers assert that controls exist but do not enforce those controls or act in a way that corroborates their supposed existence. Others appear to have no controls on their data selling and sharing whatsoever. In the course of our work, we have purchased individually identified, sensitive, and non-public data about Americans from data brokers—in compliance with our university research ethics processes—with little to no vetting from the brokers.

In recent Justice Department cases against data brokers Epsilon, Macromark, and KBM, the brokers each knowingly sold data for about a decade each to criminal scammers.[107] KBM had internal controls in place around data sales, but when an internal controller blocked the sale of consumers' data to a criminal, others in the company convinced them to override the decision and sell the information anyway.[108] In our research, we have also seen that some data brokers require clients to sign nondisclosure agreements preventing those clients from identifying where they obtained consumers' data. We have had conversations with data brokers that claim to have robust controls in place, but they have refused to provide us with any documentation to corroborate their supposed existence.

Question 19 asks, "What controls do data brokers implement to ensure the quality and accuracy of data they have collected?" Question 19(a) asks, "What controls exist related to ensuring the quality and accuracy of public records data, including court records?" Question 19(b) asks, "Are these controls adequate?" We respond:

We have seen a wide variety in how data brokers describe the accuracy and quality of the data they gather and sell. Some brokers will speak in general terms about the accuracy and

quality of their data; some brokers will provide buyers with specific assertions about accuracy and quality (e.g., "this data is at least 85% accurate"), where it is usually unclear how the numbers are calculated; and some brokers will not make claims about accuracy or quality. It is unclear if there are any internal controls related to the quality and accuracy of public records data by data brokers, though many data brokers, especially people search websites, advertise their ability to gather this kind of information. Despite a standing offer to highlight industry best-practices and internal controls around data or privacy practices, we have not been contacted by a single data broker willing to verify or prove any claims about internal controls.

Inaccurate information can be incredibly harmful to consumers. In the past, individuals have been unfairly denied credit or even erroneously labeled as a suspected terrorist due to inaccurate data.[109] The opacity of the data brokerage ecosystem—and the use of brokered data by financial institutions, private insurance (including health insurance) providers, employers, landlords, and law enforcement—means that there are numerous opportunities every day for individuals to face harm because of decisions made from brokered data. The continued persistence of credit score disputes casts doubt on the quality of internal controls even at multi-billion-dollar data brokers, like the three major credit reporting agencies, much less the parts of the data brokerage industry not under consistent regulatory watch.

Question 20 asks, "How have data broker practices evolved due to new technological developments, including machine learning or other advanced computational methods?" We respond:

Data brokers continue to evolve their business practices and technological capabilities to collect more data, infer more data, aggregate data in new ways, and market new services based on the data they hold. Many brokers advertise their ability to generate novel insights into data, such as Equifax, which provides an online platform for creating machine learning and AI insights.[110] In our research, we have received data fields labeled as "inferred," which suggest that they were produced algorithmically. The lack of accessibility of and transparency around these algorithms, however, makes it nearly impossible to judge their technical accuracy and overall merit.

Question 21 asks, "Are there companies or other entities that help consumers understand and manage their relationship to, and rights with respect to, data brokers? If not, why not? What factors could further help such consumer-assisting companies and entities?" We respond:

There are some companies that attempt to assist consumers with removing their information from people-search websites, such as DeleteMe, Incogni, IDX, and mePrism. Under the current circumstances, these companies are making important efforts to help individuals try to slightly improve the privacy of their data online. But commercializing the failures of privacy protection should not be the long-term solution to the data brokerage ecosystem's harms. Further, removing one's information from data broker websites is incredibly difficult,[111] even with these services, including because:

- Consumers do not have the right to compel data brokers to remove information pulled from government records, and the people search data brokers that provide "opt-out" forms are not legally required to let consumers opt out of the publishing of data from voting registries, property records, and other "publicly available information" sources;
- People search websites constantly repopulate their datasets, which means even if they decide to allow a consumer to remove information at one point in time, the data could simply be pulled from public records and posted again; and
- Even when people search websites attempt to comply with a filed opt-out request—again, provided by their own decision—the companies' systems may not delete every version of the webpage and may leave up links to that individuals' profile on the profiles of their friends and family members.

Stronger laws and regulations around data brokerage would not harm innovation but in fact promote responsible data practices and encourage the further development of privacy-protective data solutions that do not involve selling Americans' data.

Question 22 asks, "How might the CFPB use its supervision, enforcement, research, rulemaking, or consumer complaint functions with respect to data brokers and related harms?" We respond:

The CFPB should exercise its authority under the Fair Credit Reporting Act (FCRA) to impose more regulations on data brokers. In a February 2023 letter to CFPB Director Rohit Chopra, nonprofit advocacy groups and Senator Ron Wyden urged the CFPB to exercise its enforcement authority under FCRA § 1681s(e) and hold data brokers accountable for creating opaque markets that disproportionately deny consumers equal opportunities,

which can cause disparate impact and disparate treatment.[112] The CFPB can regulate data brokers under FCRA § 1681s(e), which prohibits the reporting of inaccurate information:

> A person shall not furnish any information relating to a consumer to any consumer reporting agency if the person knows or has reasonable cause to believe that the information is inaccurate.[113]

We would add that the CFPB can hold data brokers that inaccurately report consumer data accountable, especially if inaccurate reporting causes financial damages. This can include the reporting of student data and its impact on credit—related to the many complaints the CFPB has received about inaccurate reporting of student data increasing student debt and being hard for students to correct.[114] Many companies outside of the major three credit reporting agencies also gather and sell data about Americans' credit. The CFPB can use the definition of consumer reporting agencies under the FCRA[115]—entities engaged in a "practice of assembling or evaluating consumer credit"[116]—to regulate other data brokers taking part in these practices and putting consumers' financial opportunities and well-being at risk.

The CFPB can also use its consumer complaint function to acquire more information about potential data broker harms to individuals, which the CFPB may be better positioned than the individual—being a government agency, a regulatory body, and an entity with resources—to identify places where remedies could be introduced.

Additionally, the CFPB should use its position to ask information of data brokers, including:

- To whom they sell, license, or share data;
- How they sell, license, or share that data, such as through a login to an online portal, access to an Application Programming Interface (API), an encrypted data download, or in a spreadsheet shared via email;
- The sources from which they get data, such as mobile apps, online retailers, other data brokers, universities, employers, payment services, and lending institutions;
- The means by which they acquire data, including by building SDKs, using pixels, paying app developers for server-to-server data transfers, and scraping public sources of information;
- How they infer data points about individuals, groups, places, and behaviors;
- How data brokers re-identify supposedly "anonymous" or "de-identified" data;
- Their process of aggregating data and generating lists targeting specific demographics;
- How data about children, teenagers, poor Americans, elderly individuals, and military servicemembers is collected and sold, especially credit- and financial-related data;
- What controls they put on the use of and access to the data internally;

- How they control the selling, licensing, and sharing of the data with third parties as well as the providing of services based on that data to third parties (e.g., not supplying the data itself but allowing someone to run ads drawing on it), such as restrictions on data use, requirements for clients to disclose intended data uses, and restrictions on data reselling and resharing;
- If their controls have ever been internally ignored, deviated from, or overridden;
- What security measures they have in place to protect their data and notify consumers of breaches;
- What due diligence they conduct to ensure that clients are appropriately safeguarding the security of the data they sell, license, or share; and
- Whether they place confidentiality obligations on partners, customers, and researchers which inhibit the ability for those entities and individuals to speak with regulators and publish academic research.

The CFPB's continued work on issues related to the data brokerage ecosystem and harm to American consumers is essential, particularly as the industry's collection and sale of credit- and financial-related data grows. While the U.S. needs comprehensive federal privacy legislation—including strong controls on data brokerage, which need not wait for a comprehensive bill to be passed—CFPB regulation and oversight is a fundamentally important component of the regulatory picture.

We appreciate the opportunity to provide comments on this matter.

Respectfully signed,

Justin Sherman
Senior Fellow and Research Lead, Data Brokerage Project
Duke University Sanford School of Public Policy[117]

David Hoffman
Steed Family Professor of Public Policy
Duke University Sanford School of Public Policy

Spencer Reeves
Research and Programs Fellow
Cyber Policy Program
Duke University Sanford School of Public Policy

Aden Klein
Research Assistant, Data Brokerage Project
Duke University Sanford School of Public Policy

Brady Allen Kruse
MPP Student and Research Assistant, Data Brokerage Project
Duke University Sanford School of Public Policy

Alistair Simmons
Research Assistant, Data Brokerage Project
Duke University Sanford School of Public Policy

Hayley Barton
MPP Student and Research Assistant, Data Brokerage Project
Duke University Sanford School of Public Policy

Endnotes

[1] Consumer Financial Protection Bureau. Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information. *Federal Register*. 88 FR 16951. https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection.

[2] Justin Sherman, "The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy, and Safety," Written Testimony before the Massachusetts Legislature: Joint Committee on Consumer Protection and Professional Licensure, Hearing on Pending Legislation, June 26, 2023. https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Sherman-Justin_WrittenTestimony_MA_Legislature.pdf; Justin Sherman, "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security," Written Testimony before the House Committee on Energy and Commerce: Subcommittee on Oversight and Investigations, April 19, 2023. https://d1dth6e84htgma.cloudfront.net/Sherman_Testimony_4_19_23_b40d947a8e.pdf?updated_at=2023-04-17T17:40:42.415Z; Justin Sherman, "Data Brokerage and Threats to U.S. Privacy and Security," Written Testimony before the Senate Committee on Finance: Subcommittee on Fiscal Responsibility and Economic Growth, Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector," December 7, 2021. https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

[3] David Hoffman, "The US Innovation Economy Requires Strong National Privacy Protections," Written Testimony before the Senate Judiciary Committee, Hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation," March 12, 2019. https://www.judiciary.senate.gov/imo/media/doc/Hoffman%20Testimony1.pdf.

[4] *Response from Duke University's Data Brokerage Research Project: Federal Trade Commission (FTC) Rule on Commercial Surveillance and Data Security* (Durham: Duke University Sanford School of Public Policy, October 2022), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2022/10/Response-to-FTC-RFC-Duke-Data-Brokerage-2022.pdf.

[5] See, e.g., Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (Durham: Duke University Sanford School of Public Policy, August 2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf; Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data* (Durham: Duke University Sanford School of Public Policy, February 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf; U.S. Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability* (Washington, D.C.: Federal Trade Commission, May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[6] U.S. Senate Committee on Commerce, Science, and Transportation. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. Washington, D.C.: Senate Committee on Commerce, Science, and Transportation, December 2013. https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. ii.

[7] U.S. Federal Trade Commission, *Data Brokers: A Call for Transparency*, 20.

[8] Ibid.

[9] Alfred Ng, "Data brokers resist pressure to stop collecting info on pregnant people," *Politico*, August 1, 2022, https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988.

[10] Shoshana Wodinsky and Kyle Barr, "These Companies Know When You're Pregnant—And They're Not Keeping It a Secret," *Gizmodo*, July 30, 2022, https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426.

[11] See, e.g., Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *VICE*, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Joseph Cox, "How an ICE Contractor Tracks Phones Around the World," *VICE*, December 3, 2020, https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps; Joseph Cox, "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics," *VICE*, May 3, 2022, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[12] Pam Dixon. Testimony before the Senate Committee on Commerce, Science, and Transportation. Hearing on "What Information Do Data Brokers Have on Consumers, and How Do They Use It?" December 18, 2013. http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.
[13] Ibid.
[14] Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*; Alistair Simmons and Justin Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations," *Lawfare*, July 25, 2022, https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations.
[15] Justin Sherman, "Examining data broker Equifax's relationships with millions of employers," Duke University Sanford School of Public Policy, August 24, 2022, https://techpolicy.sanford.duke.edu/blogroll/examining-data-broker-equifaxs-relationships-with-millions-of-employers/.
[16] LexisNexis, "Public Records Search Guide," lexisnexis.com, accessed July 10, 2023, http://www.lexisnexis.com/paralegal/pubrecs.pdf.
[17] Massachusetts Office of the Attorney General, "AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities," mass.gov, April 4, 2017, https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities; Justin Sherman, "The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics," *Lawfare*, September 19, 2022, https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics.
[18] Justin Sherman, "Examining data broker Equifax's relationships with millions of employers," Duke University Sanford School of Public Policy, August 24, 2022, https://techpolicy.sanford.duke.edu/blogroll/examining-data-broker-equifaxs-relationships-with-millions-of-employers/.
[19] See: Justin Sherman, "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security," 8.
[20] Dan Rafter, "How data brokers find and sell your personal info," us.norton.com, January 18, 2021, https://us.norton.com/blog/privacy/how-data-brokers-find-and-sell-your-personal-info; Quina Baterna, "7 Types of Public Records That Data Brokers Collect," makeuseof.com, November 8, 2021, https://www.makeuseof.com/types-public-records-data-brokers-collect/.
[21] For example, see, among others, California Consumer Privacy Act — 1798.140.15.2; Colorado Privacy Act — 6-1-1303.17(b); Connecticut Act Concerning Personal Data Privacy and Online Monitoring — Section 1(18) and 1(25); Utah Consumer Privacy Act — 13-61-101.
[22] Brooke Auxier et. al, "Americans' attitudes and experiences with privacy policies and laws," Pew Research Center, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[23] Eric Griffith, "Everyone Wants Data Privacy, But No One Reads Privacy Agreements," *PC Magazine*, April 19, 2021, https://www.pcmag.com/news/everyone-wants-data-privacy-but-no-one-reads-privacy-agreements.
[24] Ibid.
[25] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* (2008), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/, 17.
[26] Ibid., 2.
[27] Kevin Litman-Navarro, "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," *The New York Times*, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.
[28] Cecilia Kang, "Flashlight app kept users in the dark about sharing location data: FTC," *The Washington Post*, December 5, 2013, https://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.
[29] U.S. Federal Trade Commission, "Flo Health, Inc.," June 22, 2021, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc

[30] Alfred Ng and Jon Keegan, "Who Is Policing the Location Data Industry," *The Markup*, February 24, 2022, https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry
[31] U.S. Federal Trade Commission, "Lurking Beneath the Surface," ftc.gov, March 16, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.
[32] Ibid.
[33] "Is Congress leaking your data to Google, Facebook, or foreign companies?," Adalytics.io, accessed July 14, 2023, https://adalytics.io/blog/is-congress-leaking-your-data.
[34] Alfred Ng and Jon Keegan, "Who Is Policing the Location Data Industry," *The Markup*, February 24, 2022, https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry
[35] Geoffrey Xiao, "Bad Bots," *Harvard Journal of Law & Technology*, Spring 2021, https://jolt.law.harvard.edu/assets/articlePDFs/v34/6.-Xiao-Bad-Bots-Regulating-the-Scraping-of-Public-Personal-Information.pdf
[36] "Mailing Lists," experian.com, accessed July 13, 2023, https://www.experian.com/small-business/mailing-lists.
[37] "Analytics and Decisioning Solutions," equifax.com, accessed July 2023, https://assets.equifax.com/marketing/US/assets/analytics_and_decisioning_brochure.pdf; "Create Your Winning Audience," americanexpress.com, accessed July 2023, https://www.americanexpress.com/us/business/amex-advance/audiences.html.
[38] Bennett Cyphers. "App Stores Have Kicked Out Some Location Data Brokers. Good, Now Kick Them All Out." EFF, March 10, 2021. https://www.eff.org/deeplinks/2021/03/apple-and-google-kicked-two-location-data-brokers-out-their-app-stores-good-now#:~:text=Data%20brokers%20entice%20app%20developers,governments%20all%20around%20the%20world.
[39] Tim Anderson, "Location tracking report: X-Mode SDK use much more widespread than first thought," *The Register*, February 3, 2021, https://www.theregister.com/2021/02/03/location_tracking_report_xmode_sdk/.
[40] Russell, N. Cameron, Joel R. Reidenberg, Elizabeth Martin, and Thomas Norton. "Transparency and the Marketplace for Student Data." SSRN, June 21, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191436.
[41] "StudentTracker," National Student Clearinghouse, April 17, 2023, https://www.studentclearinghouse.org/colleges/studenttracker/.
[42] U.S. Department of Education, last accessed June 5, 2023. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf.
[43] "Equifax Announces Industry's First Pre-Employment Verification Service Tailored to the Hourly Workforce," *Business Insider*, accessed June 29, 2023, https://markets.businessinsider.com/news/stocks/equifax-announces-industry-s-first-pre-employment-verification-service-tailored-to-the-hourly-workforce-1032398609.
[44] "Education Verification - Verify Education Status: The Work Number," Verify Education Status | The Work Number, accessed June 29, 2023, https://theworknumber.com/solutions/products/education-verification.
[45] U.S. Federal Trade Commission. *Bringing Dark Patterns to Light*. Washington, D.C.: Federal Trade Commission, September 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.
[46] *Federal Trade Commission v. Amazon.com, Inc.* (United States District Court for the Western District of Washington, 2023). https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf.
[47] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."
[48] Robert Gellman, *Without Consent 2020 - World Privacy Forum* (World Privacy Forum, 2020), https://www.worldprivacyforum.org/wp-content/uploads/2020/04/ferpa/without_consent_2020_summary.pdf.
[49] "Definition: Eligible Student from 34 CFR § 99.3 | LII / Legal Information Institute." Legal Information Institute. Accessed June 8, 2023. https://www.law.cornell.edu/definitions/index.php?width=840&height=800&iframe=true&def_id=c5d6bfea

60ed33eb6dc5028e27e718ab&term_occur=999&term_src=Title%3A34%3ASubtitle%3AA%3APart%3A99%3ASubpart%3AD%3A99.37.

[50] "Student Privacy Laws: What District & School Administrators Need To Know." Education Framework Inc - Student Data Privacy Protection for K-12 School Districts. Accessed June 29, 2023. https://educationframework.com/resources/student-privacy-laws/federal-laws.

[51] "COPPA Form Requesting That Schools/Districts Exercise Their Rights on Behalf of Parents ." Parent coalition for student privacy. Accessed July 3, 2023. https://studentprivacymatters.org/coppa-form-for-schools/#:~:text=The%20FTC%27s%20guidance%20further%20states,school%2C%20and%20for%20no%20other.

[52] Gellman, *Without Consent 2020*.

[53] Russell, N. et al., "Transparency and the Marketplace for Student Data." SSRN, June 21, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191436.

[54] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."

[55] Ibid.

[56] See, e.g., Gina Kolata, "Your Data Were 'Anonymized'? These Scientists Can Still Identify You," *The New York Times*, July 23, 2019, https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html; Omere Tene and Jules Polnetsky, "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* 11, no. 5 (2013), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip;

[57] See, e.g., Rob Matheson, "The privacy risks of compiling mobility data," Massachusetts Institute of Technology, December 7, 2018, https://news.mit.edu/2018/privacy-risks-mobility-data-1207.

[58] Bennett Cyphers, "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police," eff.org, August 31, 2022, https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police.

[59] Michael Barbaro and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *The New York Times*, August 9, 2006, https://www.nytimes.com/2006/08/09/technology/09aol.html; Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," University of Texas-Austin, 2008, https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; Marie Douriez et al., "Anonymizing NYC Taxi Data: Does It Matter?" *2016 IEEE International Conference on Data Science and Advanced Analytics* (2016), https://ieeexplore.ieee.org/document/7796899; Yongqi Dong et al., "Revealing New York taxi drivers' operation patterns focusing on the revenue aspect," *2016 12th World Congress on Intelligent Control and Automation* (2016), https://ieeexplore.ieee.org/document/7578771.

[60] Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications* 10, no. 3069 (2019), https://www.nature.com/articles/s41467-019-10933-3.

[61] *Federal Trade Commission v. Kochava Inc.* (2022). Complaint for Permanent Injunction and Other Relief. https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf. 6.

[62] Yiquan Gu and others, Data brokers co-opetition, Oxford Economic Papers, Volume 74, Issue 3, July 2022, Pages 820–839, https://doi.org/10.1093/oep/gpab042.

[63] Ibid.

[64] "Data Brokers: A Call for Transparency and Accountability: A Report Of ..." ftc.gov, 2014. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[65] Harriman, Lauren. "February 8, 2023 the Honorable Rohit Chopra Director, Consumer ..." Epic.org, 2023. https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf.

[66] See, e.g., "Verify with ID.me to Access Government Services," id.me, accessed July 14, 2022, https://www.id.me/individuals/government.

[67] Sara Morrison, "This outed priest's story is a warning for everyone about the need for data privacy laws," *Vox*, July 21, 2021, https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting; Esther Salas, "My Son Was Killed Because I'm a Federal Judge," *The New York Times*, December 8, 2020, https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html.

[68] Kim Lyons, "Congress investigating how data broker sells smartphone tracking info to law enforcement," *The Verge,* June 25, 2020, https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy

[69] U.S. Senate Committee on Commerce, Science, and Transportation. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. ii.
[70] Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*.
[71] See, e.g., "Verify, Authenticate, & Link Identities," equifax.com, accessed July 14, 2023, https://www.equifax.com/business/identity-fraud/verify-authenticate-link-identities/.
[72] Ibid.
[73] Based on our experience purchasing data from data brokers.
[74] Based on our experience purchasing data from data brokers.
[75] Based on our experience purchasing data from data brokers.
[76] Sherman, "Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security."
[77] Kaplan, Levi, Alan Mislove, and Piotr Sapieżyński. "Federal Trade Commission | Protecting America's Consumers." ftc.gov, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Kaplan-Mislove-Sapiezynski-Measuring-Biases-in-a-Data-Brokers-Coverage.pdf.
[78] Ibid.
[79] Ibid.
[80] *Katherine Sass and Cody Hounanian v. Great Lakes Educational Loan Services, Equifax Information Services, TransUnion, Experian Information Solutions, and VantageScore Solutions* (United States District Court Northern District of California May 20, 2020).
[81] H.R.748 - 116th congress (2019-2020): Cares act. Accessed June 29, 2023. https://www.congress.gov/bill/116th-congress/house-bill/748.
[82] Waggoner, John. "FAQs on the CARES Act and Student Loan Debt." AARP. Accessed June 29, 2023. https://www.aarp.org/money/credit-loans-debt/info-2020/student-loans-coronavirus-faq.html.
[83] Katherine Sass and Cody Hounanian v. Great Lakes Educational Loan Services, Equifax Information Services, TransUnion, Experian Information Solutions, and VantageScore Solutions (United States District Court Northern District of California May 20, 2020).
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] See, e.g., Andrew G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: New York University Press, 2017).
[89] See, e.g., Samantha Lai and Brooke Tanner, "Examining the intersection of data privacy and civil rights," Brookings Institution, July 18, 2022, https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights/; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: MacMillan, 2018).
[90] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."
[91] See, e.g., Aden Klein and Joanne Kim, "Data Brokers, Police, and the Criminalization of Abortion," *Tech Policy Press*, October 18, 2022, https://techpolicy.press/data-brokers-police-and-the-criminalization-of-abortion/; Sherman, "The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics."
[92] Kim, *Data Brokers and the Sale of Americans' Mental Health Data*.
[93] Michelle Boorstein and Heather Kelly, "Catholic group spent millions on app data that tracked gay priests," *The Washington Post*, March 9, 2023, https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.
[94] See, e.g., Jon Keegan and Alfred Ng, "Gay/Bi Dating App, Muslim Prayer Apps Sold Data on People's Location to a Controversial Data Broker," *The Markup*, January 27, 2022, https://themarkup.org/privacy/2022/01/27/gay-bi-dating-app-muslim-prayer-apps-sold-data-on-peoples-location-to-a-controversial-data-broker.
[95] See, e.g., *"How Dare They Peep into My Priavte Life?"* (New York: Human Rights Watch, May 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.
[96] See, e.g., Justin Sherman, "The Open Data Market and Risks to National Security," *Lawfare*, February 3, 2022, https://www.lawfaremedia.org/article/open-data-market-and-risks-national-security. The data brokerage research team also looks forward to publishing its forthcoming report on the topic.
[97] Based on our experience purchasing data from data brokers.

[98] Kim, *Data Brokers and the Sale of Americans' Mental Health Data*.
[99] Justin Sherman. "Data Brokers and the Data Breaches." Tech Policy @ Sanford, September 27, 2022. https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/
[100] Simmons, Alistair. "Data Brokers and the Sale of Students' Data." Tech Policy @ Sanford, July 10, 2023. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-students-data/.
[101] See, e.g., Delaware H.B. 262 (2021-2022), https://legis.delaware.gov/BillDetail/79022.
[102] Justin Sherman, "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," *Lawfare*, April 8, 2021, https://www.lawfaremedia.org/article/federal-privacy-rules-must-get-data-broker-definitions-right.
[103] Laura Mahoney, "California to Create Data Broker Registry, Fines for Failure," Bloomberg, October 12, 2019, https://news.bloomberglaw.com/privacy-and-data-security/california-to-create-data-broker-registry-fines-for-failure.
[104] "Data Broker Registry: Incomplete Registrations - Pending 2023 Payment," oag.ca.gov, accessed July 5, 2023, https://oag.ca.gov/data-brokers/incomplete/2023.
[105] Ibid.
[106] Forthcoming report.
[107] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."
[108] Ibid.
[109] Lawrence Hurley, "U.S. Supreme Court curbs TransUnion 'terrorist list' lawsuit," June 25, 2021. https://www.reuters.com/legal/government/us-supreme-court-limits-damages-transunion-terrorist-list-lawsuit-2021-06-25/
[110] "Analytics and Decisioning Solutions," equifax.com, accessed July 2023, https://assets.equifax.com/marketing/US/assets/analytics_and_decisioning_brochure.pdf
[111] See, e.g., Mara Hvistendahl, "I Tried to Get My Name off People-Search Sites. It Was Nearly Impossible," Consumer Reports, August 20, 2020, https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/.
[112] Harriman, Lauren. "February 8, 2023 the Honorable Rohit Chopra Director, Consumer ..." Epic.org, 2023. https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf., 1.
[113] "15 U.S. Code § 1681s–2 - Responsibilities of Furnishers of Information to Consumer Reporting Agencies." Legal Information Institute. Accessed June 7, 2023. https://www.law.cornell.edu/uscode/text/15/1681s-2.
[114] Student Data & Student Debt - files.consumerfinance.gov. Accessed May 31, 2023. https://files.consumerfinance.gov/f/documents/201702_cfpb_Enrollment-Status-Student-Loan-Report.pdf.
[115] "CFPB to Supervise Credit Reporting." Consumer Financial Protection Bureau, July 16, 2012. https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-to-superivse-credit-reporting/.
[116] CFPB consumer laws and Regulations FCRA. Accessed May 30, 2023. https://files.consumerfinance.gov/f/documents/102012_cfpb_fair-credit-reporting-act-fcra_procedures.pdf.
[117] In accordance with an academic intellectual independence policy, all signatories on this document sign in their personal, not institutional, capacities.