Duke SANFORD | CYBER POLICY PROGRAM

Response from Duke University's Data Brokerage Research Project

Federal Trade Commission (FTC) Rule on Commercial Surveillance and Data Security

October 2022

Introduction and Summary of Comments

The data brokerage research team at Duke University's Sanford School of Public Policy welcomes the opportunity to comment on the Federal Trade Commission (FTC)'s advance notice of proposed rulemaking on Commercial Surveillance and Data Security.[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.

In this comment, we describe for background purposes:

- How to define data brokerage: Data brokerage includes a broad diversity of companies and business models. Some of these companies appear to invest in significant controls and regulatory compliance efforts. However, others appear to operate with minimal controls even when processing highly sensitive information. It is important that any definition of data brokerage covers the diversity of these business models and levels of controls. The two state laws focused on data brokers, one in California and one in Vermont, define data brokers, generally speaking, as companies that sell information pertaining to individuals with whom they have no direct business relationship. Our research program takes a broader, and in some ways more intuitive, view: if a company brokers data, it is engaged in data brokerage. One possible definition of data brokerage is the collection, aggregation, analysis, buying, selling, and sharing of data, irrespective of the company's relationship with the consumer whose data is being sold or monetized. This understanding of data brokerage aligns with the FTC's previous analyses of data brokers.
- How data brokerage requires more regulation: The few privacy laws the U.S. has enacted are focused on how some entities in a few select industries or sectors use specific kinds of data. For example, the Health Insurance Portability and

[1] Federal Trade Commission. Trade Regulation Rule on Commercial Surveillance and Data Security. *Federal Register*. 87 FR 51273. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

Accountability Act (HIPAA) applies to only 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. Other laws, including those at the state level, similarly fail to place meaningful restrictions on data brokerage.

Then, we respond to specific FTC questions:

- How some data brokerage harms consumers: Data brokers collect, analyze, aggregate, sell, license, and otherwise share data about individuals that is, in some cases, highly sensitive and, in many cases, highly susceptible to abuse. The individuals whose data is being collected, aggregated, and monetized often have little to no knowledge that this data brokerage is even happening—let alone any comprehensive understanding of who is acquiring data about them and what those actors are doing with it. Collecting much of this data without appropriate controls may itself be invasive, and may expose individuals to potential harm. Data brokers have sold information to companies, criminal scammers, and abusive individuals, inflicting harm on people or enabling harm to people that includes predatory corporate profiling, theft from vulnerable individuals, and stalking and domestic violence. The extent to which data brokers place controls on the sale and use of their data is unclear, though many data brokers offer readily downloadable data without any kind of buyer verification. Several data brokers in recent years have exposed hundreds of millions of people's information through lax security practices that resulted in data breaches or data leaks.
- How commercial surveillance harms children and teenagers: Companies are legally allowed to sell, share, license access to, and otherwise monetize data they gather about children. Broadly, it is easy to go online and find data brokers advertising datasets on teenagers. Allowing this data brokerage ecosystem to persist without significant controls enables companies to legally surveil people from the moment they are born (or even before that) all the way through their adolescence, adulthood, and end of life.
- How to balance costs and benefits: The very same, narrow regulatory structure that enables relatively innocuous or even helpful uses of data through data brokerage—like verifying a current address on an apartment application or whether someone qualifies for a military discount—is the same structure that also enables great harm to consumers, including through predatory advertising, secretive profiling, stalking, scamming, and more. While some companies choose not to use consumers' data in a harmful manner, not all actors make this choice; regulators cannot trust every actor brokering data or acquiring brokered data will do so in an unharmful manner. And

companies citing what they see as relatively benign or helpful *uses* of consumers' data does not mean there are not invasive uses of that same information and that there should not be restrictions on the initial *collection* of that information.

- How to regulate data brokerage: The U.S. needs a comprehensive regulatory approach to data brokerage. In some cases, the policy response should include restrictions or outright bans on the sale of certain categories of information, such as GPS, location, and health data. In other cases, the policy response should entail restrictions on the collection, sale, and sharing of information, such as with financial data that may be used for some narrowly approved activities (like credit scoring) but which is widely collected, sold, and exploited beyond that purpose. A regulatory approach that tackles harmful uses of data after they occur fails to protect consumers. In many cases, once the data is collected and sold, shared, or used, the harm has already occurred, and it's too late.
- How to understand consent: Consumer consent is not an effective**,** administrable, or viable approach to the regulation of commercial surveillance. 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 problems 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 misrepresented 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 show that consumers do not have the knowledge, understanding, or time to shoulder this burden of self-protection.
- How the FTC should require disclosure of data brokerage practices: The FTC's list of existing questions should be supplemented with others, including:
    - to whom companies 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;
    - their process of aggregating data and generating lists targeting specific demographics;
    - 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 those entities and individuals' ability to speak with regulators and publish academic research.

We support the FTC's continued attention to these important issues of commercial surveillance, data security, and the risks and harms to American consumers.

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, 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 and 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.

Defining Data Brokerage

The two state laws focused on data brokers, one in California and one in Vermont, define data brokers, generally speaking, as companies that sell information about individuals with whom they have no direct business relationship.[2] In other words, a company that only sells information about its own customers is not considered a data broker under the California and Vermont registry laws. Federal and state bills around data brokerage frequently reflect this distinction.

Our research program takes a broader, and in some ways more intuitive, view: if a company brokers data, it is engaged in data brokerage. One possible definition of data brokerage is the collection, aggregation, analysis, buying, selling, and sharing of data,[3] irrespective of the company's relationship with the consumer whose data is being sold or monetized. The logic is that there are some companies that make data brokerage their entire business model. Other companies engage in data brokerage even though it is not their primary means of making money. Although the two types of entities make different percentages of their

[2] California Civil Code Title 1.81.48. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article=; Vermont Statute 9 V.S.A. § 2430. https://legislature.vermont.gov/statutes/section/09/062/02430.

[3] Justin Sherman. "Data Brokerage and Threats to U.S. Privacy and Security." 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.

revenue from brokering data, both categories of companies are in the business of profiting off the collection, buying, and selling (or other monetization) of consumers' data. The companies engaged in this practice range from companies publicly advertising themselves as data brokers, to companies who broker data but call themselves advertisers or marketing businesses, to mobile applications that brand themselves as providing a particular product (like a weather app or family safety app) while non-transparently selling data on their users to make a profit.

This understanding of data brokerage aligns with the FTC's previous analyses of data brokers. In the Commission's 2012 report, the FTC noted a possible distinction between "(1) entities that maintain data for marketing purposes; (2) entities subject to the FCRA [Fair Credit Reporting Act]; and (3) entities that may maintain data for other, non-marketing purposes that fall outside of the FCRA."[4] In its 2014 report, it defined data brokers as "companies that collect consumers' personal information and resell or share that information with others."[5] Again, companies that sell data on their own customers were still considered data brokers.

By failing to account for the spectrum of companies brokering data, state and federal privacy legislation has excluded some data brokers from the legal discussion and from regulation. For example, *The Markup* uncovered in December 2021 that "family safety app" Life360 was secretly selling precise location data on its parent and child users—and in 2020 made almost 20 percent of its revenue from this brokerage.[6] Despite the fact that Life360 was selling data on its own users, it would not have to register as a data broker under the California and Vermont registry laws. As a result, policy and legal regulations that use a narrow definition of data brokers will not comprehensively address the spectrum of data brokerage activities ongoing today. Companies involved in data brokerage in some capacity have a strong financial interest in limiting the scope of legal, regulatory, and policy activities vis-à-vis "data brokers" for precisely this reason.

[4] U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: Federal Trade Commission, March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, 65.

[5] 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,i.

[6] Jon Keegan and Alfred Ng, "The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users," *The Markup*, December 6, 2021, https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

The Regulatory Gap

Data brokerage is mostly unregulated. The few privacy laws the U.S. has enacted are focused on how some entities in a few select industries or sectors use specific kinds of data. For example, the Health Insurance Portability and Accountability Act (HIPAA) 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.

At the state level, the California and Vermont data broker laws do not place any restrictions on the collection, aggregation, analysis, packaging, buying, selling, and sharing of consumer data. They are registry laws, meaning they primarily force companies that fit a narrow definition of a "data broker" to submit some information to the state. (Even within that limited scope, registry information sometimes appears outdated, duplicated, or with broken links.) Some state privacy bills, like a data broker registry bill in Delaware and the Michigan state legislature's new privacy bill, would expand on the narrow definition of data broker used in the California and Vermont laws.[7] However, they also do not place strong controls on data brokerage. Other state privacy laws, such as the Virginia and Colorado laws, allow consumers to opt out of the sale of their information but provide numerous exceptions, including for data that does not match the definition of "personal data" and for "publicly available information."[8] They do not place strong controls on the business of data brokerage itself, and their do-not-sell provisions place the burden on consumers to try to marginally address systemic surveillance practices.

[7] Delaware H.B. 262. https://legis.delaware.gov/BillDetail/79022; Michigan S.B. 1182. https://www.legislature.mi.gov/(S(yiquhvromywxgybpxwrgpa4u))/mileg.aspx?page=GetObject&objectname=2022-SB-1182.

[8] Virginia Title 59.1 Chapter 53. Consumer Data Protection Act. https://law.lis.virginia.gov/vacode/title59.1/chapter53/; Colorado S.B. 21-190. Colorado Privacy Act. https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

Question category A asks, "To what extent do commercial surveillance practices or lax security measures harm consumers?" We respond:

Data brokers collect, analyze, aggregate, sell, license, and otherwise share data about individuals that is, in some cases, highly sensitive and, in many cases, highly susceptible to abuse. The individuals whose data is being collected, aggregated, and monetized often have little to no knowledge that this data brokerage is happening—let alone any comprehensive understanding of who is acquiring data about them and what those actors are doing with it. Collecting much of this data without appropriate controls may itself be invasive, and may expose individuals to potential harm. Data brokers have sold information to companies, criminal scammers, and abusive individuals, inflicting harm on people or enabling harm to people that includes predatory corporate profiling, theft from vulnerable individuals, and stalking and domestic violence. It is unclear to what extent data brokers place controls on the sale of their data, though many data brokers offer readily downloadable data without any kind of buyer verification. Several data brokers in recent years have exposed hundreds of millions of people's information through lax security practices that resulted in data breaches or data leaks (discussed more below).

Our research at Duke University has identified data brokers advertising highly sensitive information on hundreds of millions of Americans, including their demographic information (such as race, religion, gender, and income level), political preferences and beliefs, and whereabouts and GPS locations. Data brokers also advertise datasets specifically containing information on survivors of domestic and intimate partner violence, elderly individuals, people with Alzheimer's, students, first responders, healthcare workers, government employees, and current and former members of the U.S. military.[9] Investigative journalists, industry experts, and researchers have published numerous other reports over the years exposing data brokers gathering and selling people's information. 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."[10] 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

[9] 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://sites.sanford.duke.edu/techpolicy/report-data-brokers-and-sensitive-data-on-u-s-individuals/.

[10] 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.

single parenthood and the stresses of urban life on a small budget"), and other datasets targeting marginalized or vulnerable individuals with low incomes.[11] 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."[12] Much of this is sensitive.

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.[13] 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."[14] 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.[15] 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.[16] 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.[17]

The initial collection of this information can be invasive. Many consumers are not aware that when they provide their geolocation to a weather app or enter their medical information into a health app, that first-party collector may be sharing that information with third parties or monetizing it beyond the application itself (such as by selling the data to data brokers). There is not widespread public awareness about data brokerage, and data brokers often do not

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

[12] Ibid.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] Ibid.

advertise their practices to the affected consumers. Even if consumers were aware of this practice, that does not eliminate the invasiveness. Data related to race, ethnicity, religion, age, gender, sex, sexual orientation, marital status, income level, political beliefs, political cause donations, health conditions, mental health conditions, and other characteristics is highly sensitive and is easily used to identify people by name with unique combinations of those characteristics. 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.[18] 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.[19] The FTC's recently announced lawsuit against data broker Kochava states 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."[20] 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.

Companies and bad actors have used this information to harm consumers. For decades, "people search websites" have enabled domestic and intimate partner violence by scraping public records and making them available for search and sale online. Abusive individuals have bought or obtained information on people to hunt down and stalk, harass, intimidate, harm, and even murder other people, largely impacting women and members of the LGBTQIA+ community.[21] Criminal scammers have bought information from data brokers—in some cases, where the brokers are fully aware their clients are scammers—to steal from elderly Americans, people with Alzheimer's and other cognitive health issues, and other vulnerable individuals.[22] Health insurance companies have purchased data from data

[18] 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.

[19] 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.

[20] *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.

[21] This goes back decades. See, e.g., *Remsburg v. Docusearch* (2002). https://casetext.com/case/remsburg-v-docusearch.

[22] Alistair Simmons and Justin Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations," Lawfare, July 25, 2022, https://www.lawfareblog.com/data-brokers-elder-fraud-and-justice-department-investigations.

brokers—including data on race, education level, marital status, net worth, social media posts, payments of bills, and more—to profile consumers and predict the costs of providing healthcare to those people.[23] Scammers have bought payday loan applicants' financial information, which at least one data broker illegally sold, to steal millions of dollars from those people.[24] Financial firms have used brokered data to market products to consumers that "limit or obscure their access to loans, credit, and financial services."[25] New research, investigative reporting, criminal prosecutions, oversight investigations, and regulatory actions continue to expose further harmful uses of this data.

The extent to which data brokers place controls on the sale and use of their data is unclear. 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. Arguably, based on the evidence of data brokerage-linked harms (from domestic violence to consumer exploitation to criminal scamming), there is little public evidence to suggest that all data brokers implement controls to prevent harmful uses of their data. 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.[26] 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.[27] Data brokers may also require clients to sign nondisclosure agreements preventing those clients from identifying where they obtained consumers' data.

In some cases, data brokers may sell, share, or monetize inaccurate data on people. This exposes consumers to further harm when they are not only profiled by a company, but profiled in a way they are not aware of and do not understand, with information that is not correct, and with no clear way of identifying the problem and rectifying the errors. Banks, health insurance companies, and other organizations may unknowingly buy, license access

[23] Marshall Allen, "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates," NPR, July 17, 2018, https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[24] U.S. Federal Trade Commission, "FTC Charges Data Brokers with Helping Scammers Take More Than $7 Million from Consumers' Accounts," FTC.gov, August 12, 2015, https://www.ftc.gov/news-events/news/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million-consumers-accounts.

[25] Pam Dixon, "Data Brokers, Privacy, and the Fair Credit Reporting Act." Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs. June 11, 2019. https://www.banking.senate.gov/imo/media/doc/Dixon%20Testimony%206-11-19.pdf, 1.

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

[27] Ibid.

to, or use this data without knowing or assessing its accuracy. For instance, for three weeks earlier this year, data broker Equifax sent inaccurate credit scores on millions of people to lenders.[28] Anecdotal studies and media reporting have identified ChoicePoint, Acxiom, and other data brokers selling inaccurate data on at least some people.[29] In 2002, data broker and credit reporting agency TransUnion identified consumers as likely on the terrorist watch list without bothering to verify the information beyond matching a first and last name against a U.S. Treasury Department list of terrorists, drug traffickers, and other criminals.[30] Making the information accurate does not eliminate all harm; in fact, in some cases where data brokers' data tends to be highly accurate, like with "people search websites" advertising individuals' home addresses based on property records, the harms are deadly serious. Nonetheless, the possibility of data inaccuracy adds another dimension to the potential harms inflicted on consumers by data brokerage.

Lastly, securing data brokers' data is another problem. When data brokers aggregate information on consumers and package it—whether a small data broker specializing in tracking individuals' phone locations or a large data broker with hundreds of data points on hundreds of millions of Americans—there is a risk that malicious actors target that information. In recent years, data brokers have been hacked; data brokers' clients have been hacked, with the data brokers' data then exposed; and data brokers have engaged in outright poor security practices that publicly leak their data. Just one individual incident can expose data on hundreds of millions of Americans (which has happened). Some of that data is quite sensitive. Examples include:

- Equifax was hacked, exposing 147 million people's data, including names, addresses, Social Security Numbers, and driver's license numbers (2017);[31]
- Exactis exposed 340 million people's information to the public internet through an unsecured server, including names, phone numbers, home addresses, email addresses, and religions as well as people's habits, interests, and the number, age, and

[28] Andrew Ackerman and AnnaMaria Andriotis, "Equifax Sent Lenders Inaccurate Credit Scores on Millions of Consumers," *The Wall Street Journal*, August 2, 2022, https://www.wsj.com/articles/equifax-sent-lenders-inaccurate-credit-scores-on-millions-of-consumers-11659467483.

[29] See, e.g., Kalev Leetaru, "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong," *Forbes*, April 5, 2018, https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/?sh=27c28f5d3107; Bruce Schneier, "Accuracy of Commercial Data Brokers," schneieronsecurity.com, June 7, 2005, https://www.schneier.com/blog/archives/2005/06/accuracy_of_com.html.

[30] *TransUnion LLC v. Ramirez* (2021). https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

[31] Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" CSO Online, February 12, 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

gender of people's children—though, notably, some of the data was inaccurate (2018);[32]

- Apollo was hacked and billions of data points, including individuals' emails, were compromised (2018);[33]
- LimeLeads did not set up a password for its internal server, allowing anyone to access it from the public internet, and data on 49 million people then showed up on a criminal hacking forum; the data focused on companies, supposedly for the purposes of business-to-business marketing, and reportedly included full names, job titles, and user emails as well as data on employer/company names, cities, states, ZIP codes, phone numbers, website URLs, companies' total revenue, and companies' estimated number of employees (2020);[34]
- SocialData exposed data on nearly 235 million social media profiles (which it scraped from Instagram, TikTok, and YouTube and sold, against platform terms of service) through a server configured without a password or any kind of authentication (2020);[35]
- Interactive Data had its data end up in criminals' hands, seemingly because one of the clients to whom it sold data may have been breached; the data broker gathers information on consumers that includes full Social Security Numbers, dates of birth, all current and previous known physical addresses, all known email addresses, vehicle registrations, available lines of credit, and IP addresses.[36]

Other examples underscore how data brokers' aggregation of data creates unique risks to consumers when criminal hackers have an even greater incentive to steal that compiled, prepackaged information.[37]

[32] Andy Greenberg, "Marketing Firm Exactis Leaked a Personal Info Database With 340 Million Records," *WIRED*, June 27, 2018, https://www.wired.com/story/exactis-database-leak-340-million-records/.

[33] Lily Hay Newman, "A Recent Startup Breach Exposed *Billions* of Data Points," *WIRED*, October 5, 2018, https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/.

[34] Catalin Cimpanu, "49 million user records from US data broker LimeLeads put up for sale online," *ZDNet*, January 14, 2020, https://www.zdnet.com/article/49-million-user-records-from-us-data-broker-limeleads-put-up-for-sale-online/.

[35] Paul Bischoff, "Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and YouTube," comparitech.com, August 19, 2020, https://www.comparitech.com/blog/information-security/social-data-leak/.

[36] Brian Krebs, "Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims," KrebsOnSecurity.com, August 6, 2020, https://krebsonsecurity.com/2020/08/hacked-data-broker-accounts-fueled-phony-covid-loans-unemployment-claims/.

[37] Justin Sherman, "Data brokers and data breaches," Duke University Sanford School of Public Policy, September 27, 2022, https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/.

Question 12 (in category A) asks, "Lax data security measures and harmful commercial surveillance injure different kinds of consumers (e.g., young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (e.g., health, finance, employment) or in different segments or 'stacks' of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?" We respond:

Companies in different industries use the same kind of information obtained from data brokers; for example, an anti-fraud company might buy someone's location data to understand their current whereabouts, and a predatory advertising company might buy that same information to profile vulnerable populations visiting payday loan agencies. It is not possible to cleanly draw distinctions between how different sectors use brokered data because the same data can be applied for different purposes. Data that is purchased by someone for a relatively innocuous purpose, like current home address information used to verify an apartment application, can also be used to inflict serious harm—such as abusive individuals routinely buying or obtaining home address data to stalk people, commonly targeting women and members of the LGBTQIA+ community. For this reason, when evaluating harms, the FTC should consider focusing on how data brokers are collecting, storing, and aggregating data, what kinds of data they are collecting and sharing, whether and how data brokers vet their customers, and how companies and other actors (e.g., criminal scammers, abusive individuals) are using that information once it is acquired from data brokers. A comprehensive regulatory approach will ensure that unanticipated uses of data from data brokers won't go unaddressed.

Question category B asks, "To what extent do commercial surveillance practices or lax data security measures harm children, including teenagers?" We respond:

Companies are legally allowed to sell, share, license access to, and otherwise monetize data they gather about children. A May 2022 report by Human Rights Watch identified educational technology software in 49 countries and found, in 146 of the 164 products it studied, tracking of the students' activities; in some cases, the software collected data on the children and sent the information to advertisers and data brokers.[38] The investigation into Life360 by *The Markup* found that the company was selling information on adult and child users to data brokers, though the company's policy said it did not sell data on children under the age of 13.[39] Broadly, it is easy to go online and find data brokers advertising datasets on teenagers. Allowing this data brokerage ecosystem to persist without significant controls enables companies to legally surveil people from the moment they are born (or even before that) all the way through their adolescence, adulthood, and end of life. Predictions of "success" based on data collected on adolescents can shape their future outcomes, sometimes restricting a child's opportunities.

Question category C asks, "How should the Commission balance costs and benefits?" We respond:

The very same, narrow regulatory structure that enables relatively innocuous or even helpful uses of data through data brokerage—like verifying a current address on an apartment application or whether someone qualifies for a military discount—is the same structure that also enables great harm to consumers, including through predatory advertising, secretive profiling, stalking, scamming, and more. While some companies choose not to use consumers' data in a harmful manner, not all actors make this choice; regulators cannot trust every actor brokering data or acquiring brokered data will do so in an unharmful manner. And companies citing what they see as relatively benign or helpful *uses* of consumers' data does not mean there are not invasive uses of that same information and that there should not be restrictions on the initial *collection* of that information.

For example, companies might argue that aggregated location data patterns, like when named individuals' movements are obscured in a broader heatmap, are useful for retailers to understand foot traffic patterns into and around stores—and, therefore, that there is nothing wrong with gathering and selling that data. However, this obscures several other points. The collection of someone's location information—where they are at any given point in time—is highly invasive because it maps people's movements and is difficult or impossible to "anonymize." Software development kit (SDK) packages, incorporated into the code of an application, make automated data collection easy and nearly impossible for consumers to notice. Many consumers are not aware their mobile apps might be handing off GPS data to a data broker (or that the app itself is monetizing the data outside the app). And in order for a

[38] *"How Dare They Peep Into My Private Life?": Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic* (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; Kyle Barr, "Remote Learning Software Tracked Kids' Data to Sell to Advertisers and Brokers: Report," *Gizmodo*, May 25, 2022, https://gizmodo.com/remote-learning-data-brokers-privacy-1848975202.

[39] Jon Keegan and Alfred Ng, "The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users," *The Markup*

company to sell aggregated location data patterns, some party (often that data broker) is collecting the raw location data in the first place. Consumers are therefore relying on an individual company's decision-making to prevent the sale of their individually linked, real-time location information on the open market.

Further, aggregated data can still cause harm. Brokering access to information that reveals the most popular payday loan offices in a city, for instance, could enable a predatory company to run advertisements geofenced around that area. Selling information that reveals the location of reproductive health clinics and traffic patterns could enable individuals to target those centers with harassment and violence. And the fact remains that this use case of monitoring foot traffic patterns, which some companies argue is acceptable and some would see as narrowly acceptable, is only legal in an environment that *also* enables additional exploitative uses of GPS data—including the sale of individually linked, real-time GPS information, the secret collection of GPS data on Black Lives Matter protesters to identify characteristics about them, the use of location data to let anti-abortion groups run anti-abortion ads to women sitting in clinic waiting rooms, and so on.[40]

Question category D asks, "How, if at all, should the Commission regulate harmful commercial surveillance or data security practices that are prevalent?" We respond:

The U.S. needs a comprehensive regulatory approach to data brokerage. In some cases, the policy response should include restrictions or outright bans on the sale of certain categories of information, such as GPS, location, and health data. GPS and location data is intimate, unique to individuals when viewed on the whole, and highly susceptible to abuse, including in ways that enable stalking, intimidation, and physical violence as well as the outing of LGBTQIA+ people—such as when an anti-gay website acquired the location data of a closeted priest and outed him, or when a misogynistic lawyer bought address information online about a New Jersey federal judge, went to her home, and shot her husband and shot and killed her 20-year-old son.[41] Health data is another highly sensitive category of information prone to abuse. Its sale should also be banned, particularly given that HIPAA's Privacy and Security Rules established over 25 years ago that health information is a sensitive and special

[40] Zak Doffman, "Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology," *Forbes*, June 26, 2020, https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=3a9e73044a1e; Justin Sherman, "The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics," Lawfare, September 19, 2022, https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics.

[41] Sara Morrison, "This outied 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.

kind of information that demands enhanced privacy and security protections, including limits on its use, transfer, and disclosure.

In other cases, the policy response should entail restrictions on the collection, sale, and sharing of information, such as with financial data that may be used for some narrowly approved activities (like credit scoring) but which is widely collected, sold, and exploited beyond that purpose. For example, many companies advertise prepackaged datasets on individuals burdened by debt and on the lowest-income households in the United States. Focusing on the types of data that companies broker is more likely to be effective than focusing on specific industries that use brokered data. This is also a more viable approach than attempting to identify populations most harmed by data brokerage, because many kinds of consumers are vulnerable in different ways—from Black and brown people, women, queer people, poor individuals, and elderly Americans to people with Alzheimer's and other cognitive health issues, people suffering from depression, consumers with chronic health conditions, survivors of domestic and intimate partner violence, immigrants without documentation, and veterans with post-traumatic stress disorder. Anyone who is marginalized or vulnerable in society experiences a greater risk of harm when a data broker gathers, infers, or shares their information.

A regulatory approach that tackles harmful uses of data after they occur fails to protect consumers. In many cases, once the data is collected and sold, shared, or used, the harm has already occurred, and it's too late. This is most acute with people search websites and domestic and intimate partner violence. An ex post-facto regulatory action cannot undo the harm of an abusive individual acquiring someone's location data to stalk and assault them. An ex post-facto regulatory action cannot undo the ruining of someone's life because they were outed with data related to their lifestyle and sexual activity. An ex post-facto regulatory action cannot undo the damage a scammer inflicts on elderly Americans and people with Alzheimer's because the scammer legally bought their contact information from a data broker. Put simply, the U.S. needs heavy restrictions on data brokerage to properly prevent and mitigate harms and reduce the many risks to consumers and to society. Allowing companies to collect, analyze, aggregate, and sell, share, or otherwise monetize consumers' information without regulation is only inviting harms to occur.

Question 73 (in the VI. Consumer Content category) asks, “The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?” We respond:

Consumer consent is not an effective, administrable, or viable approach to the regulation of commercial surveillance. 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 problems 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 misrepresented 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 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.[42] 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;[43] only 11% say they fully read privacy policies before agreeing.[44] 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.[45] As the authors put it, “the national opportunity cost

[42] 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/.

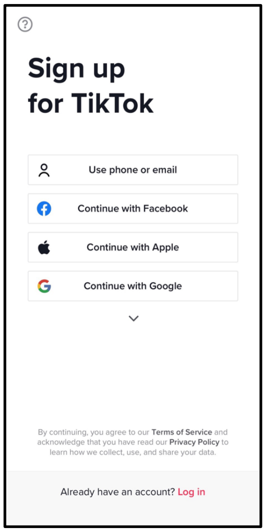
[43] Eric Griffith, “Everyone Wants Data Privacy, But No One Reads Privacy Agreements,” *PC Magazine*, April 19, 2021, https://www.pcmag.com/news/everyone-wants-data-privacy-but-no-one-reads-privacy-agreements.

[44] Ibid.

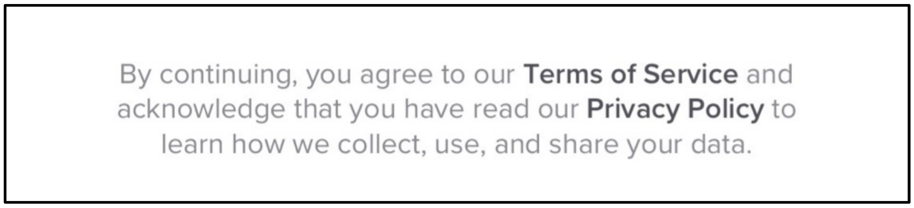
[45] Aleecia M. McDonald and Lorrie Faith Cranor, “The Cost of Reading Privacy Policies,” *I/S: A Journal of Law and Policy for the Information Society* (2008),

for just the time to read policies is on the order of $781 billion."[46] 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.[47]

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."



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.



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.

https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/, 17.

[46] Ibid., 2.

[47] 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.

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.[48]) 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 89 (in the VIII. Notice, Transparency, and Disclosure category) asks, "To what extent should trade regulation rules, if at all, require companies to explain (1) the data they use, (2) how they collect, retain, disclose, or transfer that data, (3) how they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods, (4) how they process or use that data to reach a decision, (5) whether they rely on a third-party vendor to make such decisions, (6) the impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers, and (7) risk mitigation measures to address potential consumer harms?" We respond:

The FTC should require companies to explain all of the aforementioned practices. Even if such notice is not construed as a basis for consumer consent, which it should not be, clear explanations of these practices should be required for the sake of transparency, to enable effective unfair or deceptive trade practices enforcement, and to assist those interested to

[48] 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.

attempt to understand what is going on behind the scenes with their data. Additionally, the FTC should consider requiring companies to disclose:

- 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;
- Their process of aggregating data and generating lists targeting specific demographics;
- 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 those entities and individuals' ability to speak with regulators and publish academic research.

The FTC's continued work on issues of commercial surveillance, data security, and the risks and harms to American consumers is essential as the data brokerage ecosystem continues to grow. 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—FTC 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[49]

Jolynn Dellinger
Stephen and Janet Bear Visiting Lecturer and Kenan Senior Fellow
Duke University Kenan Institute for Ethics

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

Kenneth Rogerson
Professor of the Practice and Director of Graduate Studies, MPP Program
Duke University Sanford School of Public Policy

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

Hayley Barton
MPP Student and 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

[49] In accordance with an academic intellectual independence policy, all signatories on this document sign in their personal, not institutional, capacities.

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

Anushka Srinivasan
Research Assistant, Data Brokerage Project
Duke University Sanford School of Public Policy

Joanne Kim
Young Alumni Tech Policy Fellow
Duke University Sanford School of Public Policy