DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: **TRADE-OFFS**

BY LOTHAR DETERMANN

& TEISHA JOHNSON

The authors are partners at Baker McKenzie's Palo Alto and Washington D.C.'s offices. Opinions expressed in this article are solely their own and not their firm's, clients' or others.

DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: TRADE-OFFS
By Lothar Determann & Teisha Johnson

In the ongoing debate concerning data broker regulation, tradeoffs between competition and privacy are not always holistically appreciated. This article examines the importance of data protection for individual privacy and access to data for competition , discusses the role of data brokers as to data privacy and sharing, and then reviews existing, new, and proposed regulations of data brokers. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from increased fraud, reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace.

01
INTRODUCTION

Data brokers face stiff criticism, lawsuits, actions from regulators, proposed new legislation and regulation, and political headwinds, in the United States as elsewhere.[2] Privacy advocates and journalists claim data brokers are not sufficiently regulated,[3] even though data brokers have been subject to privacy law restrictions in some of the oldest U.S. privacy laws. In the ongoing debate, tradeoffs between competition and privacy are not always holistically appreciated.

02
DATA

In an increasingly interconnected world, data is a valuable asset. No one owns data,[4] yet every business needs information to make intelligent decisions about market focus, product development, pricing, advertising, and all other aspects of running a successful company. Every online action — from liking a social media post to buying a new shirt — generates data. Companies that operate successful online presences collect lots of information that they can use to compete in their core business areas, monetize to target advertisements on their platforms, or sell to other companies or government agencies.[5] Many new market entrants and smaller businesses in particular state that they need to purchase data to compete.

03
BROKERS

Generally, brokers act as intermediaries between buyers and sellers of any item of value, including real estate, commodities, securities, and all kinds of products and services. Brokers focus on meeting demand and help optimize market dynamics, pricing, and quality. They play an important role for commerce and competition in all areas. So do data brokers. "Data brokers may provide information that can be beneficial to services that are offered in the modern economy, including credit reporting, background checks, government services, risk mitigation and fraud detection, banking, insurance, and ancestry research, as well as helping to make determinations about whether to provide these services."[6]

04
PRIVACY CONSIDERATIONS

Data brokers sell various categories of data and not all relates to individual persons. But, much of the information humans care about relates to humans and thus qualifies as "personal information" or "personal data." Under California privacy law, "data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.[7] Without a direct relationship, data brokers cannot easily inform consumers about their data collection and processing practices. From the consumer's perspective, the brokers operate "behind the scenes," collecting information from numerous sources, including e-commerce websites, social medial platforms, public records, online transactions, surveys, and more. These data collection efforts enable data brokers to amass a wide array of data and information, from basic personal details (*e.g.* names, addresses, phone numbers, email addresses) to intricate personal behavior insights (*e.g.* financial status, family connections, health conditions, details on shopping and online browsing activities, travel habits, and ge-

2 See, for example, www.cnn.com/2023/08/15/tech/privacy-rules-data-brokers/index.html.

3 See, for example, www.popsci.com/technology/data-brokers-explained/.

4 Lothar Determann, No One Owns Data, 70 Hastings Law Journal 1 (2019), available at SSRN: https://ssrn.com/abstract=3123957.

5 See, www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.

6 See, recital (d) of Assembly Bill 1202 that introduced registration requirements for data brokers in California, see https://legiscan.com/CA/text/AB1202/2019.

7 Cal. Civ. Code §1798.99.80(d).

olocation data) that can create a detailed profile of an individual. The collected data can also be aggregated and compiled into comprehensive datasets to be licensed or sold to various businesses and institutions including, advertisers, marketers, researchers, and financial institutions. The businesses that ultimately buy and use personal information about consumers often do not have relationships with the consumer either and with some of them -- e.g. collection agencies, law enforcement authorities, and telemarketers -- consumers would rather not have relationships at all. Most consumers would prefer that their data is not sold to organizations that do not wish them well or might harass them with cold calls and unwanted text messages. Most consumers also do not see any tangible upside from their data being traded by brokers. Many fear that poor data quality or hostile data usage practices could ultimately harm them. Some feel they should receive a "cut" from the profits generated with their data.[8]

05
COMPETITION CONSIDERATIONS

Without data, companies cannot effectively develop products, stock the right amount of goods in the right place, target advertisements effectively to potentially interested persons, or make informed decisions about important issues such as loans and payment terms. As the significance of data continues to increase, firms without sufficient access to data, such as new market entrants and smaller players, may not be able to effectively compete with larger, already established firms. Data brokers can play an important role in our data-driven economy by providing entities with valuable consumer insights through data selling and sharing.

However, data collection and sale can also create competition concerns if data brokers amass large amounts of unique data resulting in a data broker gaining significant market power. If access to that data set is withheld (either entirely or selectively) or if the cost of obtaining the data is so large that only a limited number of well-established data purchasers can financially purchase the data, this could create barriers to entry both for smaller firms desiring to purchase the data and for smaller data brokers attempting to enter the market as a data broker. Owning large amounts of data—particularly unique data—heightens the competition concern as there is an increased risk of the data owner taking actions to solidify its market position by behaving in anticompetitive ways that could slow innovation, cause prices to rise, reduce quality and choice, and cause other negative effects such as affecting credit decisions and how customers are treated.

Data brokers can also enhance the competitive environment and facilitate positive outcomes for consumers by embracing and facilitating the flow of data. Consumers can directly benefit from data trading where companies offer services or financial incentives to consumers in exchange for collecting information from consumers. Also, consumers can indirectly benefit, namely from effective competition, informed product development, relevant advertisements, and loan risk mitigation throughout the economy. If overly rigid data broker regulation inhibits data selling and sharing, smaller and newer companies may not have access to sufficient data to enter new product markets and compete. Without competition, companies could then solidify their market positions and raise prices, slow down innovation, deteriorate products, withhold credit, and treat consumers poorly.

06
DATA BROKER LAWS AND REGULATIONS

Fair Credit Reporting Act. Data brokers have been subject to sector-specific data privacy laws for more than 50 years in the United States. Congress enacted one of the oldest data privacy laws in the world, the federal Fair Credit Reporting Act ("FCRA"), in 1970 to regulate credit reporting agencies and provide privacy rights for personal data in consumer reports.[9] FCRA was substantially updated by the Fair and Accurate Credit Transactions Act ("FACTA") in 2003.[10] Companies have to comply with FCRA if and to the extent they act as "consumer reporting agencies," "users" or "furnishers." Most companies act at a minimum as "users" of credit reports, namely when they obtain background checks on employees or candidates. A "consumer reporting agency" is any person or entity that compiles or evaluates information on consumers for the purpose of furnishing consumer reports to third parties for a fee.[11] Equifax, Experian, and TransUnion are among the most prominent consumer reporting agencies. Other businesses that collect similar data on consumers may also be subject to the FCRA rules, depending on the purposes for which the data they sell is used.[12] "Users" are employers, lenders, insurers, and other companies that use consumer reports for various purposes.[13] "Furnishers" are companies that report information about transactions with consumers to consumer reporting agencies, such as banks or merchants that report that a debtor is late making payments. A company that furnishes only reports regarding its own transactions does not become a "consumer reporting agency," because such reports are excluded from the definition of "consumer report."[14] Friends, acquaintances and neighbors who answer requests for information from consumer reporting agencies do not qualify as furnishers either.[15]

State Privacy Laws. In 1975, California enacted the California Consumer Credit Reporting Agencies Act ("CCRAA"), with a similar focus as the federal FCRA.[16] The CCRAA regulates consumer credit reporting agencies doing business in California. More recently, states including California, Texas, Vermont, and Oregon enacted laws regulating data brokers more broadly. Vermont was the first state to require data brokers to register with the state government. California soon followed, and just this year Texas and Oregon joined California and Vermont in enacting laws regulating data brokers. The specific requirements and obligations imposed on data brokers vary by state. However, there are common themes in the regulations, including: (1) similarities in the definition of "data broker" and "personal data;" (2) the requirement that data brokers register in the state; and (3) penalties associated for data brokers who fail to register and/or provide the required information to the state. State rules also require that data brokers maintain certain security measures with respect to the data.

A. Overview of State Data Regulation Rules

Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers.[17] Vermont's law established registration, disclosure and data security requirements for data brokers trading in Vermont residents' personal information. Data brokers must register annually and adopt information security programs with appropriate safeguards to protect personal information.[18] The Vermont law defines data brokers to mean a business that "knowingly collects and sells or licenses to third parties brokered personal information of a consumer with whom the business does not have a direct relationship,"[19] and defines brokered personal information as "computerized data elements, if categorized or organized for dissemination to third parties" that include certain items about a Vermont consumer, including name, address, date or place of birth, mother's maiden name, biometric data, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information would reasonably allow the consumer's identification with reasonable certainty.[20] The law imposes civil penalties of up to $50/day (not exceeding $10,000 per year) for data brokers that fail to register.[21] As Vermont was the first state to enact data broker laws, it set a precedent which other states have followed.

> ***"Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers***

8 https://www.cnbc.com/2019/02/12/california-gov-newsom-calls-for-new-data-dividend-for-consumers.html.

9 15 U.S.C. §§ 1681–1681x. On the history of credit bureaus and regulation, see Rowena Olegario, Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development, http://documents.worldbank.org/curated/en/209261468762614853/Credit-reporting-agencies-their-historical-roots-current-status-and-role-in-market-development.

10 See 16 C.F.R. Part 682.

11 15 U.S.C. § 1681a(f).

12 LinkedIn was sued in a class action over alleged FCRA violations, but the suit was dismissed, see Sweet v. LinkedIn Corp., N.D. Cal., No. 5:14-cv-04531-PSG, 2015 WL 1744254 (N.D. Cal. April 4, 2014). Spokeo settled with the FTC on alleged FCRA violations, Stipulation for Entry of Consent Decree and Order for Civil Penalties, Injunction and Other Relief, United States of America v. Spokeo, Inc., No. CV12-05001 (C.D. Cal. June 7, 2012), available at www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeoorder.pdf.

13 See 15 U.S.C. § 1681m (requirements on users of consumer reports); 15 U.S.C. § 1681s-2 (responsibilities of furnishers of information to consumer reporting agencies).

14 15 U.S.C. § 1681a(d)(2)(A)(i).

15 16 C.F.R. § 660.2(c).

16 Cal. Civ. Code §§ 1785.1-1785.36. The law became effective in California in 1975 and has been subject to several amendments. See, for example, www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0901-0950/sb_909_cfa_20100621_110753_asm_comm.html.

17 9 V.S.A. §§ 2430, 2433, 2446 and 2447

18 See, Guidance on Vermont's Act 171 of 2018 Data Broker Regulation, 2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf (vermont.gov).

19 9 V.S.A. § 2430(4)(A).

20 9 V.S.A. § 2430(1)(A).

21 9 V.S.A. § 2446 (b).

California enacted a data broker law that looked similar (but not identical) to Vermont's data broker law. The California law requires data brokers to register every year on or before January 31 with the California Attorney General, and pay an annual registration fee.[22] In registering with the Attorney General, data brokers are required to provide its name, primary physical, email, and internet website addresses. California's data broker law borrowed many of the broad definitions from the previously adopted California Consumer Privacy Act ("CCPA") enacted in 2018, including "business," "consumer," "personal information" and "sale."[23] Companies that exchange employee or business contact information with affiliates or other business partners for consideration (monetary or other) may qualify as a business that sells personal information under CCPA; if a business does not have a direct relationship with the consumer to whom the data relates, the business may have to register as a data broker.

In September 2023, California amended its data broker law, and passed Senate Bill 362 adding additional obligations on data brokers by introducing a single "accessible deletion mechanism."[24] California consumers will be able to use the mechanism via a website maintained by the California government to request that every data broker that maintains any personal information about the consumer delete such personal information held by the data brokers or associated service providers or contractors.[25] The data brokers will be required to process deletion requests that are made through the CPPA mechanism within 31 days of receiving them, and in 2026, continuously delete the personal information of the requesting consumer and not sell or share new personal information of the consumer. Data brokers will also be required to direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the requesting consumer. The new law will require data brokers to provide additional information when registering as data brokers, including specifying whether they collect the personal information of minors, consumers' precise geolocation, and consumers' reproductive health care data.

Currently, the new California law is the first and only law giving consumers the ability to request that their data be deleted in a single request. Also, California applies the most rigid restrictions on "selling" and "sharing" of personal information in the United States and probably worldwide, applicable to businesses that have a direct relationship with consumers and who supply data to brokers and other businesses.[26] These restrictions could significantly reduce the amount of California consumer information that data brokers can trade, unless data brokers and businesses can make the case to consumers that consumers benefit from more efficient competition enabled by data trading. California privacy law also requires companies to inform consumers about the value of their personal information to the business in "notices of financial incentives" whose disclosures and terminology is dictated by prescriptive statutory requirements and regulations.[27] It remains to be seen whether these restrictions and transparency requirements will enable and enhance fair competition in data markets or stifle the data broker industry so much that smaller businesses can no longer compete with large data owners, which do not have to sell or share data.

> ***Currently, the new California law is the first and only law giving consumers the ability to request that their data be deleted in a single request***

In June, Texas signed into law a new data broker law (SB 2105) (effective as of September 1, 2023) creating registration, security, and disclosure requirements for data brokers that meet certain annual revenue or processing thresholds regarding personal data (any information that links or is reasonably able to be linked to an individual, including pseudonymous data used in combination with other identifying information).[28] Texas considers a data broker to be any business entity whose principal source of revenue is derived from collecting, processing or transferring personal data that the entity did not collect directly from the individual linked to the data.[29] Data brokers operating in Texas are required to (1) pay a fee and register with the state, (2) post language on its website or app identifying itself as a data broker, and (3) implement and maintain a comprehensive written information security program.[30] The law also outlines what must be included in the security program, including identifying risks, employee training policies, monitoring plan performance, and implementing technical safeguards around data. Violations of the law are subject to penalties of at least $100 per day, not to exceed $10,000 in one year.[31]

Oregon is the most recent state to pass a data broker registration law (HB 2052). The law was enacted in late July 2023, and similar to Vermont, California, and Texas, requires data brokers to pay a fee and register with the Oregon Department of Consumer and Business Services.[32] Oregon defines data brokers as a business entity or part of a business entity that collects and sells or licenses "brokered personal data" to another person, and broadly defines "brokered personal data" as any computerized data elements about an Oregon resident if those elements are categorized or organized for the sale of licensing to another person.[33] This includes basic information about an individual, such as name, addresses, birthdate or place, biometric information, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information that can be reasonably associated with an Oregon resident.[34] Data brokers that violate the broker registration law may face penalties up to $500 for each violation, each day (with a yearly cap of $10,000). HB2052 is set to go into effect Jan. 1, 2024.[35]

Though each state has slightly different rules, each state defines "data broker" and "personal data" broadly, requires data brokers to register, and have similar penalties for violations. While the similarities in state regulations could conceivably provide a roadmap to federal regulation, it is also possible that U.S. federal regulation of data brokers will go beyond what the states have implemented and further burden the industry with additional complexities if federal law does not preempt state laws.

B. Role of the U.S. Federal Agencies

Congress and federal agencies are becoming increasingly bullish on data broker regulation. While this is not new –there have been proposed Congressional bills and statements by federal agencies regarding data brokers over the years--the Consumer Financial Protection Bureau ("CFPB") recently announced that it plans to propose rules under the Fair Credit Reporting Act ("FCRA") requiring data brokers to comply with the FCRA.[36] The FCRA establishes data privacy requirements when consumer reporting agencies use consumer data for items such as credit and employment. The stated purpose of the to-be-proposed rules is to protect American consumers from data brokers by subjecting data brokers to greater oversight and regulation, ensuring that sensitive consumer data is protected, and preventing misuse and abuse by data brokers.

> ***Though each state has slightly different rules, each state defines "data broker" and "personal data" broadly, requires data brokers to register, and have similar penalties for violations***

In order to require data brokers comply with the FCRA, according to CFPB Director Rohit Chopra, the CFPB is considering categorizing a data broker that sells certain types of consumer data, such as a consumer's payment history, income, and criminal records as a "consumer reporting agency," thus triggering requirements to ensure

22 Cal. Civ. Code §1798.99.82.

23 See, Determann, California Privacy Law, Practical Guide and Commentary, Chapter 2C (5th Ed. 2023).

24 Cal. SB 362 (2023)

25 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/united-states-senate-bill-362-to-amend-california-data-broker-law.

26 Lothar Determann, California Privacy Law Vectors for Data Disclosures, in: *Data Disclosure: Global Developments and Perspectives*, edited by Moritz Hennemann, Kai von Lewinski, Daniela Wawra and Thomas Widjaja, Berlin, Boston: De Gruyter, 2023, pp. 121-146, https://ssrn.com/abstract=4146903.

27 https://www.connectontech.com/united-states-california-attorney-general-sets-sights-on-consumer-loyalty-programs-for-ccpa-enforcement/.

28 See Texas S.B. No. 2105 (2023).

29 See Texas S.B. No. 2105, Sec. 509.001 (2023).

30 See Texas S.B. No. 2105 (2023)

31 See Texas S.B. No. 2105, Sec. 509.008 (2023).

32 See Oregon H.B. 2052 (2023).

33 Oregon H.B. 2052, Section 1 (2023).

34 See Oregon H.B. 2052, Section 1 (2023).

35 Oregon H.B. 2052, Section 1, 7 (2023).

36 See Protecting the Public from Data Brokers in the Surveillance Industry, August 2023

that the data sold is accurate, prohibits misuse, and contains a mechanism to handle inaccurate information.[37] The rationale behind treating data brokers selling those types of consumer data as a consumer reporting agency centers around how that data is used. According to the CFPB, this type of data is typically used for credit and employment determinations, and thus should comply with the FCRA.

The CFPB and Director Chopra noted that the CFPB's rulemaking will complement other federal agencies, specifically recognizing the role of the Federal Trade Commission (FTC) as leading many efforts on privacy and data security.

The FTC has been actively involved in evaluating the conduct of data brokers for over a decade.[38] As the federal commission tasked with overseeing consumer protection, the FTC's primary concerns regarding data brokers have centered around data security, transparency, and misuse of personal information. In 2012, the FTC issued Orders requiring nine data brokerage companies to provide the agency with information about how they collect and use consumer data, specifically with respect to privacy practices.[39] That same year, they also called on the data broker industry to improve business practices by increasing transparency.[40] The FTC has continued to devote resources to gathering information about data brokers, monitoring data broker practices, and has filed suit against companies for alleged violations of the FTC Act[41] and the FCRA. The FTC views the collection, use and sale of consumer data as having the potential to cause harm to consumers due to the sensitive nature of the information collected, possible lack of protection of such data, and the potential for misuse.

The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act. The FTC has used this authority to take action against various data brokers for violations of the FTC Act consumer protection laws. The cases have resulted in significant settlements requiring data brokers to pay fines, institute tighter security measures, provide clearer disclosures to consumers, or cease operations entirely. In 2014, the FTC filed suit and agreed to settle with two data brokers on violations of the FCRA and FTC Act.[42] The allegations revolved around the use of consumer data without notifying consumers that their information was being reported, and without ensuring accuracy.[43] The FTC also published an extensive report calling for transparency and accountability for data brokers.[44] In this report, the Commission recommended that Congress consider enacting legislation to regulate data broker practices, and allow consumers to have more rights and access to their data. The key findings in the report emphasized the limited control consumers have over their personal data. The collection of data, often without consumer knowledge, can flow through multiple layers of data brokers, allowing data to be exchanged between brokers, and leading to multiple levels of data brokers storing, accessing, and making inferences about consumers based on this data.[45] All harms that the FTC would like to protect against.

> ***The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act***

While Congress has not enacted legislation based on the FTC's recommendation, the FTC continues its pursuit against alleged consumer harms caused by data brokers. In 2016, the FTC issued an Order settling charges against a data broker operation who was alleged to have fraudulently collected and sold consumer data without their consent, in violation of the FTC Act, resulting in a $7 million harm.[46]

In the past year, the agency has reconfirmed its commitment to protecting sensitive consumer data, including geolocation and health data, promising that protecting consumer data is a top priority.[47] The FTC also warned that they are committed to using the "full scope" of their authority to enforce the law against illegal use and sharing of highly sensitive data.[48] To emphasize the point, the FTC filed a complaint alleging that a location data broker engaged in unfair or deceptive acts in violation of the FTC Act when it acquired consumer's geolocations data and utilized this data to track consumer's movements and locations.[49] The complaint alleged the data broker sold precise geolocation data associated with unique identifiers revealing consumers visits to sensitive locations, and that the data broker employed "no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations." [50] The lawsuit claimed the sale of the highly sensitive data put consumers at significant risk and would likely cause substantial injury. The FTC sought to stop the sale of the sensitive geolocation data by permanently barring the data broker from selling consumer data in the future and requiring the company to delete the data it has collected. The case was dismissed, ordering that while the FTC's legal theory of consumer injury was plausible, the FTC had not made sufficient factual allegations to proceed. To do so, it must not only claim that the practices could lead to consumer injury, but that they are likely to do so.[51] In response, the FTC filed an amended complaint that currently is under seal.

The setback has not deterred the FTC from staying at the forefront of the data broker regulation efforts. The agency has shown that it will not hesitate to go after companies for alleged misuse of consumer data, including the collection, retention, and exchange or sale of this sensitive data. To accentuate the point, in late September, 2023, speaking at the 2023 Consumer Data Industry Association Law & Industry Conference, the Director of the FTC's Bureau of Consumer Protection voiced his concern with data brokers looking to "maximize" data at the cost of the consumer, posing serious risks. [52]

It is clear that there will continue to be scrutiny and enforcement around data brokers. Though the federal landscape lacks a comprehensive regulatory framework, the FTC has become the federal agency leading the charge against alleged violations by data brokers, and individual states have taken the initiative to introduce and pass legislation regulating data brokers.. As the economy evolves and data becomes an even more invaluable commodity, we can expect to see new state and federal laws regulating data brokers.

> ***It is clear that there will continue to be scrutiny and enforcement around data brokers***

37 See Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, August 2023.

38 See Data Brokers: A Call for Transparency and Accountability, 2014; and FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information | Federal Trade Commission.

39 See Order to File Special Report.

40 See FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, March 2012.

41 15 U.S.C. §§ 45(a) et. al.

42 See Consent, U.S. v. Instant Checkmate, Inc.; and see, U.S. v. Infotrack Information Services, Inc.

43 See Complaint, U.S. v. Infotrack Information Services, Inc. (2014).

44 See Data Brokers, A Call for Transparency and Accountability, FTC, May 2014.

45 See Data Brokers, A Call for Transparency and Accountability, FTC, May 2014.

46 See Stipulated Order, FTC v. Sequoia One, LLC (Nov. 2016)

47 https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

48 https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

49 *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Complaint).

50 *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Complaint).

51 See, *FTC v. Kochava Inc.*, Case No. 2:22-cv-00377 (Memorandum Decision and Order), May 24, 2023

52 https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

07
CONCLUSIONS AND OUTLOOK

Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Established businesses with large amounts of data do not have to sell or share their information and could rely less on data purchases. Similarly, data brokers that amass large amounts of unique data can pick winners and losers if they decide to whom they will and will not sell their data. Legislators will need to be thoughtful about data broker regulations—if regulation creates barriers to easy entry, it can put smaller players at a competitive disadvantage, resulting in data being consolidated into the hands of few. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace. As regulators continue to evaluate the impact of data brokering on both privacy and competition, this discourse will continue to evolve.

> *Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs*