DATA BROKERS IN THE HOT SEAT: A CONTINUING STORY

BY
JESSICA L. RICH

Of Counsel and Senior Policy Advisor for Consumer Protection, Kelley Drye & Warren LLP. Former Director, Bureau of Consumer Protection, Federal Trade Commission.

TechREG CHRONICLE
OCTOBER 2023

Visit www.competitionpolicyinternational.com for access to these articles and more!

DATA BROKERS IN THE HOT SEAT: A CONTINUING STORY
By Jessica L. Rich

For years, policymakers have debated whether new laws are needed to restrict the practices of data brokers – companies that collect consumers' data from various sources, process and package it, and then sell it to individuals and businesses for marketing and advertising, fraud detection, risk mitigation, and locating people, among other purposes. Supporters of stronger laws argue that data brokers operate behind the scenes, collecting and selling sensitive consumer data to a vast array of purchasers, who use it to make important decisions about consumers. Opponents argue that data brokers provide valuable services that help businesses and the government serve the public. Until recently, regulation of data brokers in the U.S. has been limited. During the past couple of years, however, there's been flurry of regulatory activity affecting data brokers at the federal and state levels. Of particular note, last month, California passed a new law (the Delete Act) that will allow consumers, in one step, to delete the data that all data brokers in the state have collected about them and to prevent future sales of their data. This article examines the recent regulatory activity surrounding data brokers and predicts continued focus on this industry as we move to 2024.

01 INTRODUCTION

For years, policymakers have debated whether new laws are needed to "rein in" the practices of data brokers – companies that collect consumers' personal data from various sources, process and package it, and then sell it to individuals and businesses for marketing and advertising, fraud detection, risk mitigation, and locating people, among other purposes.

Proponents of stronger laws cite data privacy and accuracy concerns, noting that most data brokers operate behind the scenes, unknown to consumers, and sell personal data (some of it highly sensitive) to a vast array of end users, who may use it to make important decisions about consumers. Data brokers counter that they provide valuable services that help businesses serve their customers, and help the economy operate efficiently and effectively.

To date, regulation of data brokers has been limited at both the federal and state level. Recently, however, there's been flurry of regulatory activity related to this industry, driven in part by the increased focus on data privacy concerns more generally. Whether in Congress or state legislatures, at federal agencies or the White House, many policymakers are pushing in the direction of increased regulation. This article provides an overview of the issues and recent activity surrounding data brokers, and forecasts stormy weather ahead for these companies.

02 WHAT ARE DATA BROKERS?

There's no universal definition of data brokers, especially since people with different perspectives tend to describe data brokers quite differently. For example, one data broker describes its business as follows:

> We unlock[] the power of data to create opportunities for consumers, businesses and society. At life's big moments – from buying a home or car, to sending a child to college, to growing a business exponentially by connecting it with new customers – we empower consumers and our clients to manage their data with confidence so they can maximize every opportunity. We help individuals take financial control and access financial services, businesses make smarter decision and thrive, lenders lend more responsibly, and organizations prevent identity fraud and crime.[2]

In contrast, a consumer advocacy group describes data brokers this way:

> Thousands of data brokers in the United States buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. As the data broker industry proliferates, companies have enormous financial incentives to collect consumers' personal data, while data brokers have little financial incentive to protect consumer data. For these companies, consumers are the product, not the customer. Companies also maintain information about consumers that is often inaccurate, wrongfully denying them credit, housing, or even a job.[3]

In a 2014 report to Congress, the Federal Trade Commission ("FTC") (the primary consumer protection agency at the federal level, with jurisdiction over many data brokers) described data brokers somewhat more objectively as "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud."[4]

Meanwhile, California's new data broker law (SB 362, discussed in more detail below) defines a data broker as "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."[5] This definition (echoed in other federal and state laws and bills) underscores one of the key issues driving concerns about data brokers – that they operate behind the scenes, collecting

2 Large data broker's website. (I'm not naming the company to avoid singling out any one data broker. Other companies' narratives are similar.)

3 Electronic Privacy Information Center (EPIC) website, https://epic.org/issues/consumer-privacy/data-brokers/.

4 FTC Report, Data Brokers: A Call for Transparency and Accountability ("FTC Data Broker Report"), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (May 2014). Although this report is almost a decade old, it is still widely cited due to its in-depth examination of the practices of nine diverse data brokers.

5 SB 362 §1(c), https://legiscan.com/CA/text/SB362/2023.

and selling consumers' sensitive data without most consumers' knowledge or control.

However data brokers are described or defined, they essentially collect, combine, process, and sell consumer data. They obtain this information from a range of sources, including government databases (e.g. real property and court records), publicly available sources (e.g. social media, blogs, and the internet), and commercial entities (e.g. retailers and magazine publishers). Often, they use online tools to collect the information, such as cookies, pixels, fingerprinting, application programming interfaces, or software development kits. They then combine the data, make inferences from it, and classify consumers by demographics, household income, familial status, political affiliation, hobbies, and other characteristics and preferences. A range of purchasers (individuals, businesses, and government) typically access data broker services online, and use it to find and authenticate people, detect and prevent fraud, and send consumers relevant advertising and offers, among other purposes.[6]

03

BACKGROUND ON THE DATA BROKER DEBATE

The debate about whether and how to regulate data brokers started in the 1960s, when concerns arose about a particular type of data broker (consumer reporting agencies or "CRAs") that collect and sell consumer information for use in making decisions about consumers' eligibility for certain benefits (notably, credit, employment, and insurance). The concerns centered primarily around three issues: (1) the confidentiality of the information collected, which included consumers' credit histories, financial status, and even data about arrests and "general reputation," (2) the accuracy and currency of the information, since false or outdated information can lead to the denial of important consumer opportunities, and (3) the fact that this system of critical decision-making had been "built up with virtually no public regulation or supervision."[7]

In 1970, Congress passed the Fair Credit Reporting Act ("FCRA"), the nation's first commercial privacy law, to address these concerns. The FCRA imposes data privacy and accuracy requirements on CRAs that sell, and on people or entities that furnish and use, consumer data ("consumer reports") for consumer eligibility determinations (i.e. about credit, employment, insurance, and other specified benefits). Among other things, the law requires CRAs to implement "reasonable procedures" to maintain data accuracy, to allow access to consumers reports only by those with a "permissible purpose," and to discard outdated information. It also gives consumers the right to review and dispute the accuracy of the information collected about them.[8] The FCRA is considered the "mother" of commercial privacy laws in the US (described admiringly by one of my former FTC colleagues as the "magna carta" of privacy).[9]

The FCRA didn't end the discussion about data brokers, however. Since its enactment, there has been explosive growth in the data broker industry,[10] with many data brokers performing services that fall outside (or purport to fall outside) the FCRA.[11] As a result, critics of the industry have pressed for broader regulation – arguing that data brokers collect highly sensitive consumer data (about consumers' health, precise location, purchase histories, family members, etc.), make inferences and assign consumers to marketing categories ("financially challenged," "leans left," "bible lifestyle"), and sell this data with few limitations. Critics also point to use of this data by the government, contrary to civil liberties, and even stalkers, who can buy their victims' addresses online. These concerns have intensified as the ubiquity of mobile devices and technological advances have enabled data brokers to collect more detailed consumer data, and make more granular inferences and predictions, for sale to the public.[12]

In response, data brokers cite the many beneficial services they provide – such as stopping fraud against companies and the government, verifying identities for the administration of unemployment and nutrition programs, identifying potential donors for charitable and political campaigns, and allowing small businesses to reach a large customer base.[13] They also argue that existing laws already govern their use of data, and are sufficient to address any harms that occur. Notably, the FCRA (as discussed) regulates the use of data for eligibility determinations; the Gramm-Leach-Bliley Act ("GLBA") protects sensitive financial information;[14] numerous state privacy laws[15] now provide a range of privacy protections in those states; and the FTC Act gives the FTC broad and flexible authority to target data brokers that engage in "unfair or deceptive" practices.[16]

04

THE CURRENT FOCUS ON DATA BROKERS

Recently, the focus on data brokers has escalated, fueled by the increased, bipartisan focus on privacy in general[17] and, the sizeable growth of the data broker industry. For some policymakers, the Supreme Court's overturning of *Roe v. Wade* has added another important dimension to the debate – i.e. the worry that law enforcers in anti-abortion states will be able to purchase data about women's health and location in order to enforce anti-abortion laws. On August 15, the White House convened a roundtable of government officials, academics, advocates, and other experts to discuss "harmful data broker practices" which provided further impetus for regulation.[18] Here are some highlights illustrating the flurry of recent activity surrounding data brokers:

A. State Data Broker Registry Laws

Over the last few years, four states have enacted data broker registry laws (California, Vermont, Texas, and Oregon),[19] with Texas and Oregon doing so just this year. All of these laws require registration with the state, submission of information, and payment of a registration fee, subject to penalties. Beyond that, the laws vary, for example, in how they define "data broker," what information must be submitted to the state, and whether the information must be disclosed to the public. While the requirements in these laws are not enormously onerous, the passage of two news ones just this year (approved by wide margins) is notable. Even more significant, California just amended its data broker registry law (via SB 362) to add a range of strict new requirements.

B. California's SB 362

In brief, SB 362[20] would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information. This request would in turn trigger an ongoing obligation for data brokers to delete any new information received about the consumer every 45 days, to refrain from selling any further information about the consumer unless the consumers opts in, and to direct any service providers or contractors also to delete the information.

6 See e.g. FTC Data Broker Report, supra at n. 4; Congressional Research Service Report R47298 ("CRS Report"), https://crsreports.congress.gov/product/pdf/R/R47298l (Oct. 2022).

7 See e.g. National Consumer Law Center Digital Library website, https://library.nclc.org/book/fair-credit-reporting/141-overview.

8 FCRA, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

9 Since enactment, the FCRA has been amended several times and has been actively enforced by the FTC, private plaintiffs, and, more recently, the Consumer Financial Protection Bureau (CFPB).

10 In 2021, digital marketing company Web FX estimated that there were over 4000 data brokers worldwide in an industry valued at more than $200 billion per year. See Web FX blogpost, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (2021).

11 Some data brokers post disclosures stating that they are not CRAs and that purchasers cannot use their data for CRA purposes. Critics say that the data is used for such purposes anyway. See CFPB Press Release, CFPB Kicks Off Rulemaking to Remove Medical Bills from Credit Reports ("CFPB Rulemaking Proposal"), https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-rulemaking-to-remove-medical-bills-from-credit-reports/ (Sept. 21, 2021).

12 See e.g. FTC Data Broker Report, *supra* at n. 4; CRS Report, *supra* at n. 6.

13 See, e.g. Consumer Data Industry Association Website, https://notosb362.org/.

14 GLBA, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act.

15 As of this writing, 12 states have enacted comprehensive data privacy laws that apply to data brokers along with other businesses. See US State Privacy Legislation Tracker, International Association of Privacy Professionals ("IAPP State Law Tracker"), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Sept. 15, 2023).

16 FTC Act, https://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I.

17 In the late 1990s, the FTC was virtually the only agency in the country addressing privacy issues, often facing opposition or skepticism from Congress. Today, multiple policymakers and enforcers at the federal and state level focus on privacy, with rising bipartisan support, greater public awareness of the issue, and privacy in the headlines every day.

18 See White House Press Release, https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/16/read-out-of-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/?utm_source=link (Aug. 16, 2023).

19 See https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article (CA); https://sos.vermont.gov/corporations/other-services/data-brokers/ (VT); https://capitol.texas.gov/tlodocs/88R/billtext/pdf/SB02105F.pdf (TX); https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/HB2052/Enrolled (OR).

20 SB 362, https://legiscan.com/CA/text/SB362/2023.

Additionally, the law would allow an "authorized agent" to request deletion for the consumer, require independent compliance audits every three years, and mandate regular reports to the public and to California's privacy regulator (the California Consumer Protection Agency). Due to the broad definition of "data broker," the bill would cover a wide array of entities, including members of the advertising industry that sell consumer data and have no consumer relationship.

The effects of this law could be quite sizeable. On the one hand, it gives consumers significant new deletion and opt-out rights that they can exercise easily, in one step. On the other hand, it raises the potential that large numbers of consumers might opt out *en masse*, whether on their own or through "authorized agents" – a prospect that could substantially impact the data broker and advertising industries, as well as the businesses and other clients that rely on them.[21] In addition, because California typically leads the states on privacy issues, it is possible that other states will follow suit, amplifying these effects considerably.

Not surprisingly, opposition to the bill among industry members was strong, with a large business coalition setting up a website for the purpose of opposing the bill (but with little success).[22] One silver lining for data brokers is that most of the law's new substantive requirements do not take effect until 2026 or even 2028.

> ***In brief, SB 362 would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information***

C. Congress

Congress, too, has been scrutinizing data brokers. For example, the leading comprehensive federal privacy bill (the bipartisan American Data Privacy and Protection Act or ADPPA) contains strict provisions that (like SB 362) require data brokers to register and comply with a one-stop-shop mechanism allowing consumers to delete data and prevent further collection by all data brokers.[23] Other recent federal bills (e.g. the bipartisan DELETE Act[24]) would impose similar requirements.

In April of this year, the Republican-led House Energy and Commerce Committee, as part of its deliberations on the ADPPA, held a hearing specifically on data brokers, making clear that committee members support strong regulation.[25] The Committee followed up in May with inquiry letters to multiple data brokers, which it announced in a press release stating (not so subtly) "E&C Leaders Continue Bipartisan Investigation into Data Brokers' Potential Exploitation of Americans' Privacy."[26] While the ADPPA is still pending in the House, the Committee's focus on data brokers is notable.

Some members of Congress are particularly concerned about government purchases from data brokers, believing that such purchases may bypass or undermine Fourth Amendment protections against unreasonable search and seizure.[27] Accordingly, over the past two years, several bills have been introduced in Congress[28] (all entitled "The Fourth Amendment is Not for Sale Act") that would require a court order, warrant, or subpoena (depending on the circumstances) for government purchases of consumers' location and web browsing and search history from data brokers. Similarly, earlier this year, some members of the House added an amendment to the National Defense Authority Act bill to restrict such purchases by the Department of Defense.[29] All of these efforts are pending, with passage uncertain, but they show mounting bipartisan efforts to place restrictions on the sale of consumer data by data brokers.[30]

D. Federal Trade Commission

Since Congress enacted the FCRA in 1970, the FTC has actively enforced it. In the late 1990s, the FTC also started to focus on the data practices of non-CRA data brokers, beginning with a report it released on "Individual Reference Services," a term then used for non-CRA data brokers.[31] Since then, the FTC has brought law enforcement actions against these companies (using its authority to police "unfair or deceptive" practices),[32] released a comprehensive report detailing their data practices (discussed above),[33] and proposed data broker legislation to Congress at least twice.[34]

More recently, the FTC has stepped up its scrutiny of data brokers, focusing in particular on the sale of health, location, and other sensitive data, and taking the position that sale of this data without consumer permission is an "unfair" practice under the FTC Act. In a blogpost last year, a senior FTC official warned that the FTC will use the "full scope of its authorities" to stop the "illegal use and sharing" of consumers' location, health, and other sensitive data, including by data brokers.[35] Soon after, the FTC filed a lawsuit against data broker *Kochava*, alleging that its sale of location data obtained from mobile devices harms consumers and is legally "unfair" because the data can reveal sensitive locations consumers visit, such as reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.[36]

The FTC also has launched a rulemaking process, with the goals of limiting "commercial surveillance" and requiring companies to implement stronger security controls in their

21 Note that the comprehensive laws that have now been passed in 12 states require many businesses, including data brokers, to provide consumers with deletion rights and the ability to opt out of sales and/or sharing with third parties. However, SB 362's more demanding requirements – including its creation of a centralized deletion and opt-out mechanism, the continuing obligation to delete, and the empowerment of "authorized agents" – are likely to have a more impact on the industry.

22 See *supra* n. 13.

23 See H.R. 8152, https://www.congress.gov/bill/117th-congress/house-bill/8152/text. The bill uses the term "third party collecting entities" in lieu of data brokers.

24 See S. 2121, https://www.congress.gov/bill/118th-congress/senate-bill/2121/text?s=1&r=9&q=%7B%22search%22%3A%5B%22Ossoff%22%5D%7D.

25 House Energy and Commerce Committee Press Release, https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers (April 19, 2023).

26 House Energy and Commerce Committee Press Release, https://energycommerce.house.gov/posts/e-and-c-leaders-continue-bipartisan-investigation-into-data-brokers-potential-exploitation-of-americans-privacy (May 10, 2023).

27 Federal laws limit the government's ability to obtain consumer data from phone companies and other providers without a warrant, court order, or subpoena. Further, the Supreme Court has held that the government's acquisition of a person's cell phone records from a wireless carrier (which can reveal a person's precise location over time) is a 4th amendment protected search, requiring a warrant supported by probable cause. *Carpenter v. US*, 585 U.S. – (2018). However, according to press reports, the government routinely gets around these restrictions by purchasing consumer data from data brokers, rather than seeking it directly from the providers. See e.g. Byron Tau, *How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies*, Wall Street Journal, https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202 (Nov. 18, 2021)

28 See S. 1265, https://www.congress.gov/bill/117th-congress/senate-bill/1265/text; HR 4639, https://judiciary.house.gov/committee-activity/markups/hr-1631-hr-4250-and-hr-4639.

29 NDAA Amendment 256, https://www.congress.gov/amendment/118th-congress/house-amendment/256/text?s=a&r=2.

30 Even the intelligence community (traditionally a major customer of data brokers) has raised concerns about government access to commercial data sources, especially data brokers. In a recently declassified report for the Director of National Intelligence, a senior advisory group discussed the increased availability of consumers' sensitive data, the privacy and civil liberty implications, and the need for more rigorous processes to safeguard and limit government use of this data. See ODNI Senior Advisory Group Report, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf. (Jan. 27, 2022).

31 FTC Report, Individual Reference Services: A Report to Congress, https://www.ftc.gov/reports/individual-reference-services-report-congress (Dec. 1997).

32 See, e.g. FTC Press Release, Sequoia One LLC, https://www.ftc.gov/news-events/news/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million-consumers-accounts (Aug. 12, 2015); FTC Press Release, Choicepoint, Inc., https://www.ftc.gov/news-events/news/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers-personal-data-left-key-electronic (Oct. 19, 2009).

33 FTC Data Broker Report, *supra* at n. 4.

34 *Id*. See also FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy (Mar. 26, 2012).

35 FTC Blogpost, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal (July 2022).

36 FTC Press Release, Kochava, Inc., https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other (Aug. 29, 2022). The court dismissed the FTC's initial complaint due to the hypothetical nature of the injury alleged, but the FTC filed a new one, which is pending and under seal.

businesses.[37] While the FTC's proposal is at a preliminary stage, it is replete with references to data brokers and data sales, suggesting that this could be a focus of any rule the FTC proposes. In addition, on September 21, a top FTC official delivered a hard-hitting speech to the leading data broker trade group, detailing the harms caused by unfettered data sales and promising more enforcement.[38]

Like Congressional efforts, the FTC's actions here are pending but show a growing effort to restrict the practices of data brokers.

> ***In brief, SB 362 would add to the registration requirements already in place by establishing an "accessible deletion mechanism" where consumers can direct data brokers to delete their information***

E. Consumer Financial Protection Bureau

Finally, in what could be the most consequential data broker regulation of all, CFPB Director Rohit Chopra announced (in mid-August, on the same day as the White House roundtable) that the CFPB would soon launch a rulemaking to "modernize" the FCRA so that it reflects how today's data brokers "build even more complex profiles about our searches, our clicks, our payments, and our locations" and "impermissibly disclose sensitive contact information" of people who don't want to be contacted, such as domestic violence survivors.[39] Then, on September 21, the agency released an outline describing its proposal, which, if ultimately implemented, could fundamentally alter the way data brokers are regulated in this country.[40]

Among the proposals that the CFPB is considering and seeking comment on are amendments to the FCRA that would bring within its scope:

(1) A data broker's sale of certain types of data (e.g. payment history, income, criminal records) because such data is "typically" used to make the eligibility determinations covered by the FCRA (i.e. decisions about consumers' eligibility for credit, employment, and other specified benefits). In other words, *any* data broker that sells this type of data would need to comply with the FCRA's strictures, including by limiting use of this data to the FCRA's "permissible purposes" and giving consumers the opportunity to dispute the accuracy of the data.

(2) Credit header information (identifying information typically included with a consumer report, such as name, address, SSN, and phone number), a major source of information for data brokers that has long been considered to fall outside the FCRA. In other words, this data, too, would be subject to all of the FCRA's data accuracy and privacy procedures.

(3) Targeted marketing that a CRA performs on behalf of clients, if consumer report data is used. Per the CFPB, CRAs may incorrectly believe that this activity isn't covered by the FCRA if the CRAs don't share the data with their clients.

(4) Household level data, or even data that is aggregated at a broader geographic level. This would be a major change as well.

Such amendments (and there are many others in the CFPB's lengthy proposal) would extend the FCRA's reach to a much broader class of data brokers than are currently covered, and dramatically limit how data brokers of all types collect and sell consumer information. The CFPB is at an early stage in the process, however.

37 FTC Web Page, Commercial Surveillance and Data Security Rulemaking, https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

38 Sam Levine, Speech at Consumer Data Association Law and Industry Conference, https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf. (Sept. 21, 2023).

39 CFPB Press Release, Remarks of CFPB Director Rohit Chopra at White House Roundtable, https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/. (Aug. 15, 2023).

40 CFPB Rulemaking Proposal, *supra* at n. 10.

05
WHERE DOES THIS LEAVE US?

If you're a consumer, you now have an increasing number of rights when it comes to data brokers, including those afforded under state data registry laws and California's SB 362. You also may soon gain additional rights through actions by the FTC, the CFPB, Congress, and additional states.

If you're a data broker, you may be mired in uncertainty, as you grapple with new laws coming into effect, and the looming possibility of additional actions from various policymakers and enforcers.

How and to what extent consumers will exercise their new rights is uncertain, since many consumers have become numb to the many privacy notices and choices coming at them.[41] We also don't know the effect that these new laws and proposals could have on the broader function of the economy – i.e. by disrupting data broker operations and the many clients that rely on them. One thing is certain, however: longstanding concerns about data brokers have escalated in a big way, and that trend seems likely to continue for the foreseeable future.

41 Research has shown that frequent, repeated notices to consumers leads to "notice fatigue" and may cause consumers to ignore notices entirely. See, e.g. Lillian Ablon et. al, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, Rand Corp., https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf (2016).

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL