United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

2023 Consumer Data Industry Association Law & Industry Conference

Surveillance in the Shadows – Third-Party Data Aggregation and the Threat to our Liberties

September 21, 2023

Thank you for inviting me to speak today and for your warm welcome.[1] As all of you know, CDIA's work overlaps greatly with that of the FTC. On issues ranging from credit reporting to tenant screening to identity theft, we welcome the opportunity to hear from your members and engage with your organization. To that end, after my remarks I will reserve plenty of time for your questions.

While there is much I could discuss today, I want to focus on an issue of particular concern to me, to the FTC, and to the American public. That issue is unchecked commercial surveillance[2], and how that surveillance endangers our privacy, our financial welfare, and our liberty. With increasing precision, companies are collecting and sharing a staggering amount of information about American consumers. Without much cost or effort, anyone in the United States or abroad can obtain detailed information about where Americans spend their days, sleep at night, what health conditions they have, who they associate with, as well as what their religious faith and political interests are. This should concern all of us.

Today I will discuss how we arrived at this point, and in particular the failures of the notice-and-choice regime. I'll then discuss how the FTC is moving decidedly away from that regime and using all of our tools to ensure substantive protections for people's data. Finally, I hope to start a conversation about some of the distinct problems we are seeing around data aggregators, and what should be done to protect the public and avoid law enforcement scrutiny.

I. How We Got Here: Our Surveillance Economy and the Failure of Notice and Choice

Understanding where we are today requires a look back at how our current privacy regime has evolved. And the FTC played a key role. At the turn of the last century, the FTC called on Congress to pass legislation codifying certain Fair Information Practices.[3] The Commission had previously called for self-regulation of online commerce, but concluded in a major report that self-regulatory efforts were

[1] I wish to thank Elizabeth Averill and Bhavna Changrani for their substantial assistance in preparing these remarks. In addition, I am grateful to Ben Wiseman and Tiffany George for their comments and suggestions. My comments today are my own and do not necessarily reflect the position of the Federal Trade Commission or any individual Commissioner.

[2] The term "commercial surveillance" is intended to capture the reality of contemporary data collection, which rests on the pervasive and comprehensive tracking of consumers' movements and behaviors across virtually every aspect of our daily lives. This is a concept that retired Harvard Business School Professor Shoshana Zuboff helped popularize in her 2019 book: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

[3] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress* (May 2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

falling short, and that Congress needed to act to protect Americans' privacy.

Although the legislation advocated for then would likely not suffice today – indeed, it did not go nearly as far as last year's bipartisan privacy legislation – the Commission, in my view, was wise to recognize the dangers posed by unchecked collection of consumers' personal information.

But that position was short-lived. The following year – with a new Administration in place – the new Chairman of the FTC announced his view that legislation would be premature, and indicated an intent to instead have the agency focus on ensuring websites posted and honored their privacy policies.[4]

In my view, the FTC should take great pride in how – over the last three decades – we have used Section 5 to take on challenges in the digital economy, and we should be particularly proud of how we deployed our unfairness authority to tackle lax data security and other challenges. But I believe it was a serious mistake to favor self-regulation over establishing baseline but binding protections for the American public. And although the Commission later came to endorse privacy legislation,[5] that took a decade – by which time powerful interests were already lined up against laws that could limit their ability to monetize data.

With no legislation in place, what has emerged over the last two decades is a regime grounded entirely in the fiction of notice and choice. I've spoken many times before about why this regime has failed the American public, so I'll be brief here, and blunt. Consumers do not have the time to read hundreds of pages of dense privacy policies, and it should not be their burden to do so. Nor do consumers have real choice when so much of our lives depends on participating in the digital economy. The notice-and-choice regime we've lived under these last thirty years has been great for the lawyers who draft these privacy policies. What it has not done is actually protect consumers' privacy.

Nor can it be said that Americans are happy with our present state of affairs. A 2019 study found that roughly six-in-ten U.S. adults said they did not think it was possible to go through their daily lives without having data collected about them by companies or the government.[6] The same research also showed that most Americans felt concerned about the way their data was being used, and eight-in-ten adults felt they had very little or no control over how these entities used their personal information.

Notably, Americans have expressed particular concern about how their data is being monetized. Earlier this year, in research conducted at the University of Pennsylvania, 91% of respondents agreed with the statement that they wanted to have control over what marketers can learn about them online.[7] A startling 79% also agreed with a statement they had come to believe they had "little control" over

---

[4] Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond* (October 4, 2001), *available at* https://www.ftc.gov/news-events/news/speeches/protecting-consumers-privacy-2002-beyond.

[5] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) *available at* https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[6] *See* Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), *available at* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-ofcontrol-over-their-personal-information/.

[7] *See* Joseph Turow, et al., *Americans Can't Consent to Companies' Use of Their Data*, Annenberg School for Communication, University of Pennsylvania (February 2023), *available at* https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

what marketers learned about them online.[8] Taken together, such survey results suggest that American consumers – in addition to contending with typical worries like health, bills, job security, safety – are also quite worried about the ways in which their data is collected and used but feel helpless to prevent it.

That notice and choice has been a failure is no surprise to many observers. But more than ever before, leadership of the FTC is stating that plainly.[9] And that pivot isn't only rhetorical. The view that Americans need substantive safeguards for their data – rather than more disclosures – has been at the heart of the agency's approach to our privacy work over the last two years. We are using new tools and new strategies to deliver real protections for Americans' data.

II. FTC Actions to Limit Unlawful Commercial Surveillance

First, we are using our rulemaking authority to examine and address pressing privacy and data security issues. Last year, the FTC launched a rulemaking proceeding around commercial surveillance and lax data security.[10] We are currently in the process of reviewing the more than 11,000 comments as well as input from stakeholders during our public hearing, reflecting broad and deep public interest in the issues being considered. The FTC also continues its ongoing review of the COPPA Rule, where we are looking carefully at some of the provisions of COPPA that go beyond notice and choice.

Our rulemaking agenda is grounded in what we are seeing in our enforcement actions, where we are breaking new ground in securing substantive protections for consumers' privacy. Consider what we've done on health privacy. In three recent actions – GoodRx[11], BetterHelp[12], and PreMom[13] – we've charged firms with unlawfully sharing consumers' sensitive health data. Significantly, the resulting orders in these cases do more than simply require that the companies obtain consumer consent before sharing sensitive health data for advertising purposes. Instead, the orders prohibit the practice altogether.[14]

We are also taking bold action to protect children's privacy. Earlier this year, we obtained a $275 million penalty against Epic Games, Inc., for children's privacy violations, including using default

---

[8] *Id.*

[9] *See, e.g.*, *Remarks of Chair Lina M. Khan at IAAP Global Privacy Summit 2022* (April 11, 2022), *available at* https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022; *Keynote Remarks of Samuel Levine at the Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference* (May 19, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf.

[10] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).

[11] *US v. GoodRx Holdings, Inc*., 23-cv-460 (N.D. Cal. Feb. 1, 2023), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc.

[12] *In re BetterHelp, Inc.*, C-4796, *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter.

[13] *US v. Easy Healthcare Corp.,* 23-cv-03107 (N.D. Ill. May 17, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf.

[14] *US v. Easy Healthcare Corp.,* 23-cv-03107 (N.D. Ill. 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf (stip. order); *US v. GoodRx Holdings, Inc*. 23-cv-460 (N.D. Cal. 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf (stip. order); *In re BetterHelp, Inc.*, C-4796, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf. (final order).

settings that facilitated text and voice communications between young users and strangers.[15] The resulting order requires not only compliance with COPPA, but mandates strong privacy-enhancing default settings in Epic's video games to better protect children and teens. Shortly thereafter, we announced a proposed settlement with Amazon resolving allegations that the company prevented parents from exercising their deletion rights under the COPPA Rule and kept sensitive voice and geolocation data for years gathered through Alexa-related products, while putting data at risk of harm from unnecessary access.[16] The Commission has also taken action against companies for unlawful collection and retention of information from children, restricted how companies can use children's information, and required either data minimization or deletion, as appropriate.[17]

Even outside the contexts of health and children's data, an increasing number of orders in our privacy and data security cases are requiring companies to minimize the consumer data they collect and retain it for no longer than is reasonably necessary.[18] Data that isn't collected can't be compromised, and the unnecessary retention of vast troves of personal data heighten the risks and increase the stakes of data breaches, manipulation, and other abuses. What is driving this excessive collection and retention is a topic I will turn to next.

III. Data Aggregators and Data Maximization

Having criticized the notice-and-choice regime, I will now speak up in its defense: having some notice and some choice – however illusory – is better than having neither. Yet that is often the state of affairs when it comes to third-party data aggregators.

Let's start by discussing the raw material fueling this business – consumer data. The lack of federal baseline protections has meant that consumer-facing firms across our economy are engaging in vast, unfettered tracking of our behaviors. In fact, over eight-in-ten adults say they keep their smartphone near them almost all the time during their waking hours, exposing them to always-on surveillance that allows firms to track their residences, place of work, marital status, children, prescriptions, where they travel daily, and more.[19] Some of this tracking, of course, provides beneficial services to consumers – such as locating the nearest gas station when they share their location. However, much of this tracking is not intended to serve consumers, but instead to gather data that can be sold to aggregators. In this way, the data aggregator industry has essentially created a lucrative market for consumer data exhaust

---

[15] *US v. Epic Games, Inc.*, 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1923203epicgamesfedctorder.pdf (stip. order).
[16] *US v. Amazon.com, Inc. et al.,* 2:23-cv-00811-TL (W.D. Wa. July 19, 2023), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v.
[17] *See, e.g., US v. Microsoft Corp*., 2:23-cv-00836 (W.D. Wa. June 9, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/ordered_entered_6.09.2023.pdf (stip. order); *US v. Edmodo, LLC*, 3:23-cv-02495 (N.D. Cal. June 27, 2023) *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Edmodo-Dkt15%28Order%20Signed%20by%20the%20Court%29.pdf (stip. order).
[18] *See US v. Edmodo, LLC*, 3:23-cv-02495, Dkt. 15 (N.D. Cal. June 27, 2023) *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Edmodo-Dkt15%28Order%20Signed%20by%20the%20Court%29.pdf (stip. order); *In re Chegg, Inc*., C-4782 (FTC Jan. 26, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Chegg-DecisionandOrder.pdf (final decision & order); *In re Drizly, LLC.,* C-4780 (FTC Jan. 10, 2023), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2023185-drizly-combined-consent.pdf (complaint and order).
[19] *See* Lydia Saad, *Americans Have Close but Wary Bond With Their Smartphone*, Gallup (June 20, 2022), *available at* https://news.gallup.com/poll/393785/americans-close-wary-bond-smartphone.aspx.

– incentivizing consumer-facing firms to collect more and more. Industry research estimates that this market was valued at $240 billion in 2021 and is estimated to reach over $450 billion in the next ten years.[20]

Once a company has collected consumer information, consumers typically have no control over what is being done with it, how it is used, or who it is sold to next. Worse than this unchecked collection is the continuous cycle of companies buying more data on each consumer, aggregating, creating profiles, and selling these profiles to additional third parties with little screening about potential uses. Countless data aggregators collect, buy, and combine data from multiple sources and sell it to marketers, researchers, or government agencies.

This vast market for third-party data has introduced incentives that do not serve consumers well. Consumer-facing firms are incentivized to extract as much data as they can, while the third parties involved are incentivized to find new ways to monetize it, with little incentive to confirm its accuracy or restrict its resale.

The effects of these incentives are quite profound, in my view. Even as Congress and many states consider efforts to impose data minimization standards, this industry is fostering a powerful countercurrent of data *maximization*.

This fever to maximize data extraction poses serious risks. Even when intentions are benign, I have serious concerns about a business model that has led to the creation of detailed digital dossiers on almost every American. Today, I want to focus on three concerns in particular. The first and most obvious is consumer privacy – our ability to safeguard the most intimate details of our lives from surveillance – and as Justice Brandeis framed it, "the right to be let alone."[21] The second is economic participation – our ability to fully participate in the economic life of this country, from accessing healthcare to securing housing. And finally, I believe this maximization model is posing serious threats to our constitutional liberties as Americans – our freedom of worship, our freedom of assembly, and our freedom of association. I'll discuss each in turn.

A. Putting Sensitive Data at Risk

Much of the harm from the prolific trade in consumer data happens in the shadows. But what is known and public should disturb us all. In one well-publicized example, an organization used precise mobile geolocation data to identify by name a Catholic priest who visited LGBTQ+-associated locations and forced him to resign his position.[22] In other examples, journalists purchased geolocation data from a company and were able to track consumers over time and identify military officials and law enforcement officers.[23] Journalists have also tracked a woman attending a prayer service at a church and been able to confirm her identity.[24]

---

[20] *See* Transparency Market Research, *Data Brokers Market Outlook 2031* (July 2022), *available at* https://www.transparencymarketresearch.com/data-brokers-market.html.
[21] *See Olmstead v. US*, 277 U.S. 438, 478 (1928).
[22] *See, e.g.,* The Associated Press, *Priest outed via Grindr app highlights rampant data tracking*, *available at* https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493.
[23] *See* Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
[24] *Id.*

One window into this surveillance is through people search services, which are abundant, provide free or low-cost information, and make it frighteningly easy for anyone to conduct background searches, and for criminals to easily identify where victims live or are seeking shelter. Not all such free or low-cost background information is reliable or accurate. Just last week, the Commission filed a complaint and obtained a $5.8 million-dollar civil penalty against Instant Checkmate and TruthFinder, companies that sell consumer background reports, for violating the FCRA by promoting their reports for tenant and employment screening without complying with the statute, for making deceptive claims of accuracy about their background reports, for making deceptive claims that consumers have criminal records, and for making deceptive claims about consumers' ability to remove inaccurate information.[25] Although the alleged conduct is serious, it is not unusual.[26]

B. Limiting Economic Participation

It should be clear that these practices raise serious privacy concerns. But the stakes are not limited to privacy alone. Profiles containing consumer personal information, and inferences generated about consumers based on such data, are increasingly used to determine if they qualify for a loan, insurance, jobs, or an apartment lease. Consider some of the FTC's recent work around tenant screening. In 2020, we charged AppFolio, which provides background reports on consumers to thousands of property management companies, with failing to ensure that criminal and eviction records it received from a third-party vendor were accurate before including such information in its tenant screening reports. Practices like these create a real risk that consumers can unjustly be shut out of housing, and the problem has not gone away. In fact, earlier this year, the Commission, in partnership with the CFPB, sought information on background tenant screening practices, including the use of criminal and eviction records, algorithmic decision making, and how these practices affect consumers' ability to obtain rental housing.

Inaccurate or false data about consumers can also torpedo job prospects. In recent federal court litigation, individuals have detailed how inaccurate criminal history data has harmed their ability to secure employment.[27] Such error-ridden background checks furnished by background screening companies have the potential to cause great harm and financial devastation to consumers of all backgrounds.

C. Threatening Constitutional Liberties

The privacy harms posed by commercial use and misuse of consumer data are serious and well known. But it is not only commercial misuse that Americans fear. Survey evidence suggests that a large

---

[25] *FTC v. Instant Checkmate LLC, et al.,* 3:23-cv-01674 (S.D. Cal. Sep. 11, 2023) *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/truthfinder-llc-ftc-v (complaint & stip. order).
[26] *See, e.g., US v. MyLife.com Inc*., 2:20-cv-06692 (C.D. Cal. 2021) *available at* https://www.ftc.gov/system/files/documents/cases/1823022mylifestipulatedorder.pdf (stip. order)
[27] *See Henderson v. Source for Pub. Data, L.P.*, 3:20-cv-294, Doc. 56 (E.D. Va. 2020) (second amended complaint). *See also* National Consumer Law Center, *Broken Records Redux: How Errors by Criminal Background Check Companies Continue to Harm Consumers Seeking Jobs and Housing* (2019), *available at* https://www.nclc.org/resources/report-broken-records-redux/.

majority of Americans are concerned about how the government is using their data,[28] and that concern is not baseless. In fact, I believe that the ease with which the government can purchase detailed sensitive personal information about Americans can endanger rights protected by the U.S. Constitution, including freedom of religion, speech, assembly, and association, and freedom from unreasonable search and seizure.[29]

Consider the threat to our religious liberties. Collecting, analyzing, packaging, and selling datasets of consumers based on their religious affiliation and location, or their leadership positions in religious organizations, poses serious risk of chilling religious expression. And this is not hypothetical. Companies today are selling datasets with titles such as "Ethnic Insight>Religion>Catholic," "Religion>Pastors," "Demographics>Religion>Islamic/Muslim," "E-Tech>Religion>Protestant," and "B2C>Religion>Jewish."[30] Such data is being put to use in expected and completely unexpected ways. For example, it was recently reported that a county in California hired a data broker to track the number of people attending church during the COVID lockdown.[31] Alarmingly, researchers studying this industry's practices related to data on consumers' mental health conditions have discovered that datasets containing highly specific information about people's medical conditions was often paired with their religion, age, and gender.[32]

And it is not only our religious liberty that is endangered by this profiling. Consider another core right – our right to assemble and protest. When Americans fear that their protest activity can be monitored – a reasonable concern[33] – this has a clear chilling effect on their exercise of their First Amendment rights. Similar concerns about monitoring and exposure to law enforcement action may also change

---

[28] *See* Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), *available at* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-ofcontrol-over-their-personal-information/.

[29] *See* Emily Glazer and Patience Haggin, *Political Groups Track Protesters Cellphone Data*, (June 14, 2020), *available at* https://www.wsj.com/articles/how-political-groups-are-harvesting-data-from-protesters-11592156142.

[30] *See* John Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You* (June 8, 2023), *available at* https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[31] *Calvary Chapel San Jose, et al. v. Santa Clara County, et al.*, 5:23-cv-04277 (N.D. Cal. Aug 22, 2023); Gabriel Greschler, *Phone Data Surveillance Used to Monitor San Jose Church that Violated Covid Rules* (March 8, 2023), *available at* https://www.mercurynews.com/2023/03/08/phone-data-surveillance-used-to-monitor-san-jose-church-that-violated-covid-rules/ ; *see also* U.S. House Comm. on Energy & Commerce, *How Your Online Data is Being Abused to Surveil you and Violate Your Freedoms* (June 5, 2023), *available at* https://energycommerce.house.gov/posts/how-your-online-data-is-being-abused-to-surveil-you-and-violate-your-freedoms.

[32] *See* Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke Sanford Cyber Policy Program (February 2023), *available at* https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.

[33] *See generally,* Press Release, Office of Senator Wyden, *Wyden Demands Investigation of Federal Agencies Surveilling Black Lives Matter Protests*, (Oct. 15, 2020), *available at* https://www.wyden.senate.gov/news/press-releases/wyden-demands-investigation-of-federal-agencies-surveilling-black-lives-matter-protests; *see also* https://eshoo.house.gov/sites/evo-subsites/eshoo-evo.house.gov/files/Eshoo-Rush-Wyden%20ltr%20to%20PCLOB%20re%20protests%20-%2010.15.20.pdf; Douglas Perry, *Law enforcement is using aircraft to collect cell-phone, other data on protesters, 'chilling 1st Amendment rights': Dem lawmakers*, The Oregonian, (June 12, 2020), *available at* https://www.oregonlive.com/nation/2020/06/law-enforcement-is-using-aircraft-to-collect-cell-phone-other-data-on-protesters-chilling-1st-amendment-rights-dem-lawmakers.html.

the decisions that people make about their healthcare.[34]

The fact that government can easily tap into a vast commercial data marketplace suggests that the distinction between government and private surveillance is becoming increasingly blurry.

You needn't take my word for it. The Supreme Court, in its landmark *Carpenter* decision, recognized that Americans have a "reasonable expectation of privacy" in certain digital information.[35] In that decision, the Court held that the government must obtain a warrant in order to collect persistent location information, specifically, cell site location information for seven days or more.[36] The Supreme Court's analysis was clear – when data is sensitive and reveals the "privacies of life" – like your associations, habits, and beliefs - it is entitled to Fourth Amendment protections.[37]

The broad language of the opinion suggests that much of the data collected by companies is sensitive personal information and must be treated with the strictest privacy safeguards. This includes things that most Americans would prefer to keep private from their neighbors, companies, and government, including sexual preferences, religious beliefs, political leanings, and their mental or physical health status.

Even the Intelligence Community is now sounding the alarm about the government's unfettered access to commercially available data about Americans, and its potential impact on Constitutional rights.[38] A recently declassified report studying the role of commercially available information sold by data brokers noted the increased volume and sensitivity of commercially available information – a byproduct of the widespread use of smartphones and other electronic devices, and the location tracking information they generate.[39] The report acknowledged that commercially available information has increasingly important risks and implications for Americans' privacy and civil liberties, since it can reveal sensitive and intimate information about individuals, and cause harm to individuals' reputation, well-being, or physical safety.[40] The report also offered the Intelligence Community recommendations for developing a framework to establish safeguards for potential future government use of commercially available data.[41]

There is also bipartisan concern on Capitol Hill about data brokers selling consumer data to the government and how that may undermine constitutional protections prohibiting warrantless searches. In April of this year the House Energy & Commerce Committee (Subcommittee on Oversight &

---

[34] *See* Naomi Nix and Elizabeth Dwoskin, *Search warrants for abortion data leave tech companies few options*, Washington Post (Aug. 12, 2022), *available at* https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/; Geoffrey A. Fowler and Tatum Hunter, *For people seeking abortions, digital privacy is suddenly critical*, (June 24, 2022), *available at* https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/; Kashmir Hill, *Deleting Your Period Tracker Won't Protect You*, (June 30, 2022), *available at* https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html.

[35] *Carpenter v. United States*, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018).

[36] *Id.* at 521.

[37] *Id.* at 521-523.

[38] ODNI Senior Advisory Group (SAG) Panel on Commercially Available Information, *90-day Report to the Director of National Intelligence on CAI*, (January 27, 2022), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

[39] *Id*. at 11.

[40] *Id.* at 17, 22-23.

[41] *Id.* at 46-47.

Investigations) held hearings examining the role of Data Brokers in the Digital Economy.[42] These hearings examined what types of data are being sold to the government and how often, as well as the policy implications. And in June, the House Judiciary Committee advanced legislation, The Fourth Amendment is Not for Sale Act, closing loopholes that allow data brokers to sell consumer data to the government.[43] In June, we also saw the House adopt the Davidson-Jacobs amendment to the NDAA, placing limits on the Defense Department's purchase and use of data from data brokers.[44] These legislative efforts serve as an important sign to third-party data aggregators and other companies collecting and sharing consumer data that the rampant collection and sale of Americans' sensitive personal information is raising alarms across society and across the government.

IV. Where We Go From Here

You have now heard me criticize an industry that many of you participate in and advocate for. But one of CDIA's founding principles was to "promote[] the *responsible use* of consumer data" and "help[] ensure fair and safe transactions for consumer[s]." I think those are worthy goals, and I want to provide some feedback that I hope you find constructive.

Let's start with some basics. At a minimum, companies must take concrete actions to evaluate what consumer data they collect and how they collect it. That means a comprehensive assessment of what type of consumer data they collect and if it is accurate. A critical part of this analysis is determining if the consumer data collected is sensitive and implementing policies and procedures to protect such sensitive consumer data, or technical measures to avoid collecting it in the first place. Understanding how you collect data means also inspecting what consumers were promised at the time their data was collected, about how it would be used, if it would be sold, to whom, and for what purpose. This also includes understanding if consumers were tricked or manipulated through design techniques and dark patterns to give consent.

Second, companies must do more to vet the third parties they share consumer data with, ask more questions about how data will be used, and impose restrictions on downstream uses. Follow the old "trust but verify" adage. This means investing less in the use of non-disclosure agreements to limit details of such transactions, and more in know-your-customer identity verification reviews and implementing technical controls to detect misuse of data.

Third, companies must be transparent with consumers about data practices. Do you provide complete and accurate information about your data processing and retention practices? Do you provide simple to understand and easy-to-access instructions to consumers on how to take advantage of their legal rights? For the reasons I detailed earlier, transparency is not always sufficient – but it's always necessary.

---

[42] *See generally* U.S. House Comm. on Energy & Commerce, *Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy* (April 19, 2023), *available at* https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-who-is-buying-and-selling-your-data-shining-a-light-on-data-brokers.

[43] *See* Tonya Riley, *Legislation preventing data broker sales to government agencies moves forward*, Cyberscoop, (July 19, 2023), *available at* https://cyberscoop.com/legislation-data-brokers-congress-privacy-surveillance/.

[44] NDAA FY 2024, H.R. 2670, 118th Cong. amend. 1375 (2023), *available at* https://amendments-rules.house.gov/amendments/Revised%20-%20DAVIOH_060_xml230712212650854.pdf.

Fourth, you must employ robust data security practices and procedures to safeguard consumers personal information that you collect and store.

Finally, companies in the consumer reporting space must fully comply with the FCRA and related FTC and CFPB guidance.

As your industry faces increased scrutiny from consumer protection agencies, from the Intelligence Community, from Congress, and from the Supreme Court, implementing these steps could go a long way toward addressing serious concerns that are emerging across the government and across the political spectrum. And the stakes could not be higher – not only for the business model that many of you have come to rely on, but also for our privacy, our economic well-being, and our liberty.

V. Conclusion

I want to conclude by making clear that your industry plays an important role in our economy, and while I have serious concerns about many of the practices we're seeing, I hope we can work together to foster a marketplace that allows commerce to thrive without compromising Americans' fundamental rights. Throughout these remarks I have tried to be very candid with you, but this is a two-way street, and I hope that in our remaining time you can reciprocate that candor by sharing your thoughts and questions. I look forward to hearing from you.