MEMORANDUM

To: Members and Staff, Subcommittee on Oversight and Investigations

From: Majority Committee Staff

Re: Hearing on "Who is Selling Your Data?: A Critical Examination of the Role of Data Brokers in the Digital Economy"

The Subcommittee on Oversight and Investigations has scheduled a hearing on Wednesday, April 19, 2023, at 2:00 p.m. (ET), or 30 minutes after the conclusion of the Subcommittee on Communications and Technology hearing starting at 10:30 a.m. (ET), whichever is later. The hearing will take place in 2322 Rayburn House Office Building and is entitled "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy."

I. WITNESSES

The following witnesses have been invited to testify on behalf of the Republicans:

Justin Sherman
Senior Fellow & Research Lead Data Brokerage Project
Duke University Sanford School of Public Policy

Marshall Erwin
VP & Chief Security Officer
Mozilla Corporation

The following witness has been invited to testify on behalf of the Democrats:

Prof. Laura Moy
Associate Professor of Law; Faculty Director, Center on Privacy & Technology
Georgetown Law Center

II. OVERVIEW

Data brokers collect, aggregate, license, and sell a wide range of information from Americans, including, but not limited to, demographic, location, and health data. However, there are many unanswered questions about how this industry operates. Companies in this ecosystem often profit from selling Americans' personal data with little government oversight and in some cases, with minimal concern for or understanding of how the buyer intends to use the data. Meanwhile, Americans are often unaware of when data brokers have collected, purchased, sold,

or shared their data. Because the disclosure of Americans personal data can lead to significant harms, data brokers must take stronger action to protect Americans' privacy.

American privacy and data security concerns are not new, and the problem has been exacerbated by the increasing amount of data and digital information collected on individuals through apps and online services in recent years. To date, existing laws do not sufficiently protect Americans' data. Data brokers can easily circumvent existing rules and laws regarding the collection and sharing of certain types of data, such as the Health Insurance Portability and Accountability Act (HIPPA).[1] This hearing will allow members to learn more about the data broker ecosystem from privacy experts and advocates as Congress continues to debate federal privacy and data security legislation.

III. BACKGROUND

A. Data brokers

Data brokers are companies that collect personal information about consumers from a variety of sources and aggregate, analyze, sell, and share that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud.[2] In many cases, data brokers gather or purchase Americans' data from websites and mobile app developers through data collection tools such as cookies, pixels, fingerprinting, application programming interfaces (APIs), or software development kits (SDKs).[3] Once the brokers analyze and aggregate the data, they can sell, license, or share the data with clients such as marketing and advertising companies, government agencies, and independent researchers.

Additionally, data brokers may not be taking the necessary steps to protect Americans' privacy and sensitive information. For example, a recent study from Duke University found that "some data brokers are marketing highly sensitive data on individuals' mental health conditions on the open market, with seemingly minimal vetting of customers and seemingly few controls on the use of purchased data."[4] Also, data brokers and their clients may be able to use location and other data to directly target and harm individuals. In testimony before the Energy and Commerce Committee in June 2022, one witness noted that, "Location data can be combined with other data to reveal an individual's movements or to track them in real time, which can pose a significant

---

[1]Sherman, Justin, "Data Brokerage and Threats to U.S. Privacy and Security." written testimony to U.S. Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, Hearing "Promoting Competition, Growth, and Privacy Protection in the Technology Sector" (Dec. 7, 2021);. https://www.finance.senate.gov/hearings/promoting-competition-growth-and-privacy-protection-in-the-technology-sector

[2]Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*. (May 27, 2014); https://www.ftc.gov/news-events/news/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more-transparent-give-consumers-greater

[3]Cho, Clare Y. and Kristen E. Busch, "Online Consumer Data Collection and Data Privacy." Congressional Research Service. R47298. (October 31, 2022); https://www.crs.gov/reports/pdf/R47298/R47298.pdf

[4]Kim, Joanne, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford School of Public Policy (Feb. 13, 2023) https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-americans-mental-health-data/

threat to physical safety."[5] The witness also stated, "Despite common assurances from companies, precise location data is not "anonymous" and can in many cases be linked back to an individual."[6] For example, during government-enforced COVID-19 lockdowns, Santa Clara County Officials used mobile phone data, collected by a data broker, to spy on Californians exercising their right to attend church services.[7]

Americans frequently do not have control over their own personal data nor the ability to stop the unchecked vacuuming up of their most sensitive private information; they cannot control how their private sensitive information is shared, sold, or interpreted by corporate third parties, nor can they delete or correct their own personal data after it has been collected. According to the Electronic Privacy Information Center's (EPIC)'s comments on a recent Federal Trade Commission (FTC) proposed data security regulation, the overcollection and secondary uses of personal data, including the sale to and use by data brokers, are inconsistent with the reasonable expectations of online consumers and may lead to discriminatory targeting that violates the privacy and autonomy of consumers.[8]

Further, Americans are often unaware of when data brokers have collected, purchased, or sold their sensitive information. In March 2023, the FTC voted 4-0 to fine BetterHelp, an online counseling service, $7.8 million for failing to safeguard private, sensitive mental health data.[9] BetterHelp, despite promises to users it would not disclose private health data (except in limited circumstances) shared user email addresses, IP addresses, and health questionnaire information to Facebook, Snapchat, Criteo, and Pinterest for advertising purposes.[10]

B. Legislation and regulation

---

[5]Fitzgerald, Caitriona "Statement of Caitroina Fitzgerald, Deputy Director, Electronic Privacy Information Center (EPIC)." written testimony to U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, Hearing "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security." pg6. June 14, 2022. https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf

[6]Fitzgerald, Caitriona "Statement of Caitroina Fitzgerald, Deputy Director, Electronic Privacy Information Center (EPIC)." written testimony to U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, Hearing "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security." pg6. June 14, 2022. https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf

[7]Greschler, Gabriel, *Cell Data, Surveillance Used to Enforce County Pandemic Rules*, Government Technology. (March 9, 2023). https://www.govtech.com/health/cell-data-surveillance-used-to-enforce-county-pandemic-rules

[8]*Comments to the Federal Trade Commission: Proposed Trade Regulation Rule on Commercial Surveillance and Data Security, R111004.* "Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem." Electronic Privacy Information Center. (Nov. 21, 2022); https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf

[9]Federal Trade Commission, *FTC to Ban Better Help from revealing Consumer Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising* (Mar. 2, 2023); https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

[10]Federal Trade Commission, *FTC to Ban Better Help from revealing Consumer Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising* (Mar. 2, 2023); https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

Current laws and regulations are not sufficient to protect Americans' data. The United States relies on a patchwork of sector-specific privacy-related federal statutes that establish varying degrees of protection, impose different collection and use limitations on various entities, and provide consumers with varying degrees of individual rights.[11] These laws include the Health Insurance Portability and Accountability Act, which protects information collected by a health care provider;[12] the Family Educational Rights and Privacy Act, which regulates the collection of student data by public school officials and those they designate;[13] the Children's Online Privacy Protection Act of 1998 (COPPA), which covers data for children 12 and under with respect to online services directed to children;[14] the Genetic Information Nondiscrimination Act, which prohibits misuse of genetic data in employment or insurance decisions;[15] and the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, which apply to financial institutions and credit reporting agencies.[16] However, many different types of data and entities are not covered by those or other sector specific laws.

The FTC has limited authority under Section 5 of the FTC Act to litigate unfair and deceptive corporate practices that mislead Americans about their data practices, so companies are allowed to set their own rules for collecting and selling data in most instances.[17] This means that there is not a direct requirement for data brokers to prioritize privacy, which can inevitably harm Americans. Also, according to recent testimony before this Committee, the current "notice and consent" approach is inadequate to protect modern technology users given the complexity of privacy policies and the importance of many online services.[18]

Further, state laws passed in recent years targeting the data broker industry have created a patchwork of new requirements which leads to conflicting and confusing obligations on businesses that are often difficult to comply with and provide different rights to consumers on how they can control their own data. Since California enacted the California Consumer Privacy Act (CCPA) in 2018, four states (Virginia, Colorado, Utah, and Connecticut) have enacted their own language with differing provisions, and more proposals continue to surface in other states, as well as California continuing to expand on its current statute. Therefore, a uniform and comprehensive national data privacy and security standard would codify consumers' data protection rights and prevent companies from collecting, processing, and transferring unnecessary data, hiding behind incomprehensible terms of service, or misusing personal information.

---

[11]Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, Seattle University Law Review (Apr. 9, 2019).
[12]Health Insurance Portability and Accountability Act, Pub. L. No. 104-191.
[13]20 U.S.C. § 1232g.
[14]15 U.S.C. § 6501, et seq.
[15]Genetic Information Nondiscrimination Act, Pub. L. No. 110-233.
[16]15 U.S.C. §§ 6801-6809; 15 U.S.C. § 1681 et seq.
[17]15 U.S.C. § 45.
[18]Reeve Givens, Alexandra "Testimony of Alexandra Reeve Givens, President & CEO, Center for Democracy & Technology." written testimony to U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Innovation, Data, and Commerce, Hearing "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." Pg. 7-8. (Mar. 1, 2023). https://cdt.org/wp-content/uploads/2023/02/HHRG-118-IF17-Wstate-GivensA-20230301-final.pdf

In the 117th Congress, the Committee on Energy and Commerce passed H.R. 8152, the American Data Privacy and Protection Act (ADPPA) to provide Americans with foundational control over their data privacy, require strong data security practices from businesses, create strong oversight mechanisms, and establish meaningful enforcement.[19] This law would directly regulate the data broker industry to protect Americans' data privacy rights, and this hearing would help further inform the Committee's efforts to debate and pass bipartisan comprehensive privacy and data security legislation. Further, the Subcommittee on Innovation, Data, and Commerce held two hearings in the last year on Americans' privacy, and data security with leading privacy think tanks, activists, and industry experts.[20] This hearing would build upon these previous hearings and focus directly on the harms of the data broker ecosystem.

IV. KEY QUESTIONS

The hearing may include discussion around the following key questions:

1. What data elements do data brokers collect on customers and market to clients?
    a. In particular, what health, location, phone, or purchase history data do data brokers collect and market?
    b. What are the typical sources of these data?

2. Do data brokers take any additional precautions to protect American's data and guard against the misuse of particularly sensitive data elements or types of data?

3. Do data brokers take any additional steps to protect children's data?

4. What notice and/or opportunity for consent or opt-out do data brokers give to the individuals whose data they are purchasing or selling?

5. How, if at all, do data brokers vet clients when licensing or selling data?
    a. Are there any policies on how clients may use the data once it has been licensed or sold?
    b. What data and how often do data brokers sell or license to government clients, in particular law enforcement agencies? What other legal or policy issues does this raise for Americans?

6. Do data brokers typically deidentify the data they provide to clients, and is identifiable data available?

---

[19]H.R. 8152 – American Data Privacy and Protection Act. 117th Congress. House Energy and Commerce Committee. https://www.congress.gov/bill/117th-congress/house-bill/8152/text

[20]Committee on Energy and Commerce, Subcommittee on Innovation, Data, and Commerce hearing entitled "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security." June 14, 2022 https://energycommerce.house.gov/events/protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security; Committee on Energy and Commerce, Subcommittee on Innovation, Data, and Commerce hearing entitled "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy" March 1, 2023 https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy

a. If data brokers provide deidentified data, what steps do they take to deidentify data?
b. What kind of procedures do data brokers have in place to ensure that a client does not use the data to re-identify an individual?

7. How have recent state privacy laws on data brokers, including those in California and Vermont, affected data brokers policies and practices?

    a. Are these state laws sufficient in protecting privacy?
    b. How does the American Data Privacy and Protection Act compare or interact with these laws?

8. What protections do data brokers have in place to ensure that data is not sold to, or shared with, foreign adversaries, or companies beholden to foreign adversaries including China, Russia, North Korea, and Iran?

V. STAFF CONTACTS

For questions regarding the hearing, please contact Deep Buddharaju, or Michael Steinberg with the Subcommittee on Oversight and Investigations Majority staff at (202) 225-3641.