CATHY McMORRIS RODGERS, WASHINGTON
CHAIR

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

May 10, 2023

Mr. Lee M. Shavel
President & CEO
Verisk Analytics
545 Washington Boulevard
Jersey City, NJ 07310-1686

Dear Mr. Shavel:

Data brokers purchase, collect, aggregate, license, sell, or otherwise share a wide range of information from Americans, including but not limited to demographic, location, and health data. These companies profit from trading in Americans' personal information, including sensitive information, often with little government oversight and, in some cases, without any concern for how buyers use the consumer data that they provide. A recent study from Duke University found, for example, 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."[1] Because the disclosure of personal data can lead to significant harms, the Committee is investigating the role that Verisk and others have played in eroding Americans' data privacy.

Americans are often unaware when third parties have purchased, collected, aggregated, licensed, sold, or otherwise shared their sensitive information. Recently, the Federal Trade Commission (FTC) voted 4-0 to require BetterHelp, an online counseling service, to pay $7.8 million for failing to protect users' health information after promising to keep sensitive mental health data private.[2] BetterHelp provided people's email addresses, IP addresses, and health questionnaire information to Facebook, Snapchat, Criteo, and Pinterest to use for advertising purposes despite promising consumers that it would not use or disclose their personal health data

[1]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/

[2]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

except for limited purposes. It also claimed that it was in compliance with the Health Insurance Portability and Accountability Act (HIPAA) by putting a deceptive "HIPAA Compliant" seal on its website.[3] This is but one example of how companies have abused their users' data for their own commercial benefit.

American privacy concerns in the data broker industry are not new, and existing laws do not sufficiently protect Americans' data from misuse. In 2014, the FTC issued a report recommending that Congress require data brokers to increase transparency and give Americans more control of their data.[4] However, data brokers can easily circumvent existing rules and laws regarding the collection and sharing of certain types of data, such as HIPAA.[5]

Enacting a comprehensive federal privacy law is a top priority for the Committee on Energy and Commerce. Currently, Americans do not have control over whether and where their personal data is sold and shared; they have no guaranteed way to access, delete, or correct their data; and they have no ability to stop the unchecked collection of their sensitive personal information. According to the Electronic Privacy Information Center, 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.[6]

To assist in advancing the Committee's understanding of the data broker ecosystem and the information your companies are purchasing, collecting, using, licensing, or selling, we request you respond to the following by no later than May 24, 2023:

1) What data elements do you collect or possess on Americans and market to your clients?
    a. In particular, do you collect or possess any of the following:
        i. Americans' health data? If yes, what kind of health data?
        ii. Americans' location data? If yes, what data elements?

---

[3]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

[4]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

[5]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

[6]*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

iii. Americans' phone data, such as data on any apps downloaded on their mobile devices? If yes, what data elements?
iv. Information revealing Americans' purchase history? If yes, what data elements?
v. Information about children under the age of 13?
vi. Information about children between the ages of 13 and 18?

2) Are there any categories of Americans' personal information that you will not purchase, collect, aggregate, license, or sell and, if so, what categories are those?

3) When you license, sell, or otherwise share Americans' personal information with your clients, do you require your clients to disclose the purpose(s) for which they will use the data? If so, what do you do, if anything, to confirm they are using the data for the stated purpose(s)?

4) When you license, sell, or otherwise share Americans' personal information, do you place any limitations on how they can use the information you provide? If so, what are those limitations and how do you enforce those limitations? If not, why not?

5) What notice and/or opportunity for consent or opt-out options do you give to the American consumers whose personal information you are purchasing, collecting, aggregating, licensing, selling, or otherwise sharing?

6) How, if at all, do you verify that the consumer information that you purchase, collect, aggregate, license, sell, or otherwise share is accurate?

7) How much money did you spend in each of the past five years on purchasing or licensing Americans' personal information?

8) From how many sources did you acquire, purchase, or license Americans' personal information for each of the past five years?
    a. What is the average and median number of variables you purchased or licensed from each source?
    b. Are agreements with each data source customized with different terms? If so, what factors determine changes to a standard agreement?
    c. Does your company have policies and procedures for disclosing information about your buyers—including how they have historically used data that they have purchased from your company in the past—to parties from which you collect, purchase, or license data? If not, why not? If so, please describe those policies.
    d. Did any of the agreements to acquire, purchase, or license the data provide conditions on how that data must be stored, used, or transferred? If so, please describe those agreements, the data related to each, and what steps you take to ensure compliance with those conditions.

9) What percentage of your annual revenue for each of the past five years was derived from selling or licensing Americans' personal information?

10) How many clients did you sell or license Americans' personal information to?
    a. What is the average and median number of variables you sell or license to each client?
    b. Are agreements with each client customized with different terms? If so, what factors determine changes to a standard agreement?
    c. Do you require your buyers to articulate the purpose(s) for which they are purchasing or licensing data? Do you conduct any post-sales audits or follow-up to ensure that actual use of the data is consistent with the stated purpose at time of purchase?
    d. Did any of the agreements to sell, license, or otherwise transfer the data provide conditions on how that data must be stored, used, or transferred? If so, please describe those agreements, the data related to each, and what steps you take to ensure compliance with those conditions.

11) How, if at all, does your company vet clients when licensing or selling data? Are there any policies on how your clients may use the data once it has been licensed or sold?
    a. What procedures do you have in place to verify that clients are not using data to exploit or harm consumers? Have you ever identified misuse, and, if so, what were the consequences for the client? Have you ever changed your policies and procedures based on misuse of data by your buyers?
    b. Does your company have a policy regarding selling, licensing, or otherwise sharing Americans' personal information with law enforcement?

12) Does your company de-identify the data you provide to clients and is identifiable data available?
    a. If your company provides de-identified data, what steps does your company take to de-identify data?
    b. What policies and procedures, if any, do you have in place to ensure that a client does not re-identify de-identified data? Have you ever identified violations of those policies and procedures, and if so, what were the consequences for the client?

13) Does your company use the personal information of Americans that you purchase, collect, or aggregate to categorize people based on income, sex, age, race, or other categories?
    a. Please provide a list of any and all categories of users that you make available for sale based on profiles that you build on users.
    b. Are any of these categories based on inferences derived about users based on raw data purchased from parties that directly collect that data from individuals?

14) What steps, if any, does your company take to protect data of users under 18?

15) What, if any, policy changes have you implemented as a result of California and Vermont's data broker laws?

16) What protections, if any, do you 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?

17) What protections, if any, do you have in place to ensure that neither you nor your clients sell or share Americans' personal information with individuals who are sanctioned by the U.S. government?

18) When you become aware that you or your clients have transferred Americans' personal information to a foreign adversary or a company beholden to a foreign adversary—currently defined by the Secretary of Commerce to include China, Russia, North Korea, Cuba, the Maduro regime in Venezuela, and Iran—do you notify the individual(s) whose personal information has been transferred or any U.S. government entity? If not, why not?

19) Do you store any American's personal information in any of these above-listed countries? If so, is it stored there by a company beholden to any government of the above-listed countries?

Sincerely,

Cathy McMorris Rodgers
Chair
Energy and Commerce Committee

Frank Pallone, Jr.
Ranking Member
Energy and Commerce Committee

Bob Latta
Chair
Subcommittee on Communications
and Technology

Doris Matsui
Ranking Member
Subcommittee on Communications
and Technology

Gus Bilikaris
Chair
Subcommittee on Innovation,
Data, and Commerce

Jan Schakowsky
Ranking Member
Subcommittee on Innovation,
Data, and Commerce

Brett Guthrie
Chair
Subcommittee on Health

Anna Eshoo
Ranking Member
Subcommittee on Health

H. Morgan Griffith
Chair
Subcommittee on Oversight
and Investigations

Kathy Castor
Ranking Member
Subcommittee on Oversight and
Investigations