Data Brokers: A Call for Transparency and Accountability
Matter No. P125404

Statement of Commissioner Julie Brill
May 27, 2014

[H]e that filches from me my good name
Robs me of that which not enriches him,
And makes me poor indeed.

– William Shakespeare, *Othello*

Data brokers gather massive amounts of data, from online and offline sources, and combine them into profiles about each of us. Data brokers examine each piece of information they hold about us – where we live, where we work and how much we earn, our race, our daily activities (both off line and online), our interests, our health conditions and our overall financial status – to create a narrative about our past, present and even our future lives. Perhaps we are described as "Financially Challenged" or instead as "Bible Lifestyle."[1] Perhaps we are also placed in a category of "Diabetes Interest" or "Smoker in Household."[2] Data brokers' clients use these profiles to send us advertisements we might be interested in, an activity that can benefit both the advertiser and the consumer. But these profiles can also be used to determine whether and on what terms companies should do business with us as individual consumers, and could result in our being treated differently based on characteristics such as our race, income, or sexual orientation. If data broker profiles are based on inaccurate information or inappropriate classifications, or used for inappropriate purposes, the profiles have the ability to not only rob us of our good name, but also to lead to lost economic opportunities, higher costs, and other significant harm.

Consumers are largely unaware of the existence of data brokers and the detailed, sensitive information contained in their profiles. As a result, to the extent that some data brokers offer consumers the ability to access and correct or suppress their data, consumers don't know how to exercise these rights, rendering such rights illusory. Furthermore, as detailed in the Commission's report, *Data Brokers: A Call for Transparency and Accountability*, data may change hands many times along the way from source to data product. As a result, even if consumers are aware of the existence of data brokers and their profiles, and have the ability to access the data about them, it is challenging, if not effectively impossible, for them to identify the sources of data and who else has seen it.

As the Commission outlines in today's report, many data broker practices fall outside of any specific laws that require the industry to be transparent, provide consumers with access to data, or take steps to ensure that the data that they maintain is accurate. The Commission's legislative recommendations, if enacted into law, would add transparency across the data broker industry, provide more information about the sources of data brokers' information, help give

[1] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY at 20 n.52, 21 (2014) [hereinafter DATA BROKER REPORT].
[2] *Id.* at 46, 55.

consumers appropriate access and the ability to correct data used for marketing and risk mitigation products, and give consumers greater ability to correct data in their people search profiles. In addition, the report encourages data brokers to be more accountable by conducting due diligence on their customers' use of the data, and creating contractual requirements that prohibit their customers from using the data in an unlawful manner.

I fully support the report and its legislative recommendations. In the report, the Commission describes the benefits and risks that arise in an interconnected system of data brokers, their customers and sources – some consumer-facing and some not —and their subjects – the consumers themselves. The Commission's recommendations are based on a thorough study and analysis of how these different players relate to each other, and the recommendations address risks to consumers in a coherent way. Specifically, the Commission recommends that Congress consider legislation that establishes requirements for each of the three categories of data brokers' products described in the report: marketing products, risk mitigation products, and people search products.[3] I set out my understanding of the Commission's legislative recommendations in a separate document available at http://go.usa.gov/8NpT.

For marketing products, the Commission recommends legislation that would require "the creation of a centralized mechanism, such as an Internet portal, where data brokers can identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs."[4] A centralized portal is critically important. If adopted, the portal would provide transparency across a broad swath of the data broker industry while also affording consumers greater practical control over their data. This requirement is a key element of the best practices that I have been encouraging data brokers to adopt.[5]

Also of critical importance is the Commission's call for requirements that data brokers' sources offer consumers transparency and choice mechanisms.[6] Data broker sources often collect information that consumers provide in a different context and for a different purpose. For example, a consumer who provides her name and email address to register with a travel or medical website might find that information being disclosed to a data broker and used to create an individual profile that combines information about her from many other sources. A requirement that the sources of data broker information used for marketing purposes provide consumer control over collection – express affirmative consent for sensitive information collection, notice and choice for other information – would allow consumers to prevent the collection and use of data that might harm them by blocking information from entering marketing databases in the first place.[7] Because disclosure of information to data brokers, and

---

[3] *See id.* at 48-53.
[4] *Id.* at 50.
[5] *See, e.g.*, Julie Brill, A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf; Julie Brill, Reclaim Your Name – Keynote Address to the 23rd Computers, Freedom, and Privacy Conference (June 26, 2013) *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.
[6] DATA BROKER REPORT, *supra* note 1, at 51.
[7] This recommendation to require express affirmative consent for sensitive information, and notice and choice for other information, is consistent with the Commission's 2012 privacy report. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 48-

their subsequent use of the information, often fall outside of the context in which consumers provide the information, prominent notice is appropriate. The Commission's call for transparency and choice at the source of data would enhance the ability of consumers to learn about these practices as the information would come to them from retailers, websites, social media, and other entities with which consumers are interacting.[8]

Taken together, the Commission's legislative recommendations, if enacted, would begin to build meaningful levels of transparency, access, and control into the data broker industry.

I write separately today to describe the additional legislative requirements that I believe are needed to ensure that all participants in the industry are appropriately accountable for the use of data brokers' products.

Two areas of discussion in the report demonstrate the need to build additional transparency and accountability measures into legislation. First, data brokers are not only collecting health, financial, racial, and other sensitive information about consumers, but also using other, innocuous data to predict or infer sensitive characteristics.[9] Congress has acted repeatedly to create privacy protections for health and financial data, and federal laws restrict the use of certain kinds of information in credit, lending, housing, and other contexts. Some data products discussed in the Commission's report expose some significant gaps in these laws. Some data brokers – albeit not the nine brokers that the Commission studied for this report – sell marketing lists that identify consumers with specific health conditions, such as addictions and AIDS. The report also identifies marketing segments that focus on ethnicity, financial status, and health conditions.[10] Examples of segments with apparent ethnic dimensions include "Metro Parents" (single parents who are "primarily high school or vocationally educated" and are handling the "stresses of urban life on a small budget") and "Timeless Traditions" (immigrants who "speak[] some English, but generally prefer[] Spanish").[11] Nothing in the Commission's report suggests that data brokers or their clients are running afoul of anti-discrimination laws. It is foreseeable, however, that data that closely follow categories that are not permissible grounds for treating consumers differently in a broad array of commercial transactions will be used in exactly this way.

The second area of the report that demonstrates the need for further legislative accountability requirements is its discussion of risk mitigation products. Risk mitigation products support an expanding range of decisions that could have a substantial impact on consumers' lives. For example, banks use identity verification products to meet statutory

---

50 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[8] Moreover, placing such requirements on data sources would appropriately complement legal protections that apply to other industry sectors, such as healthcare providers and financial institutions. *See, e.g.*, Health Insurance Portability and Accountability Act, 110 Stat. 1936 (establishing privacy safeguards for personal health information in certain settings); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.) (establishing safeguards that financial institutions must observe for "nonpublic personal information").

[9] DATA BROKER REPORT, *supra* note 1, at 20 & n.52; *id.* at 25 & n.57.

[10] *See id.* at 20 & n.52; *id.* at 25 & n.57

[11] *Id.* at 20 n.52.

customer identification requirements.[12] Other data broker clients use the history of transactions associated with a consumer's email address to assess whether a particular transaction is likely to be fraudulent.[13] In these ways, risk mitigation products can protect consumers and businesses.

When inaccurate information wrongly leads to a consumer being identified as a risk that needs to be mitigated, however, that consumer may suffer significant harm. The consumer may be unable to complete important transactions, such as opening a bank or mobile phone account, if the data that went into a risk mitigation product is incorrect. Moreover, the consumer may be unable to determine why a transaction was blocked, much less correct underlying inaccuracies, if she has no knowledge that risk mitigation products have been used in rendering the adverse decision. As the Commission notes in the report, enabling consumers to correct inaccurate data used in risk mitigation products should not enable consumers to "correct" truthful information or otherwise undermine broader identity protection, fraud detection, or other risk-reduction purposes. The report also notes that some data brokers have already determined how to effectively provide consumers with access and correction rights while still ensuring the integrity of their products.[14] This demonstrates that the Commission, industry, and other stakeholders should be able to address the challenge of enabling correction while preventing the subversion of risk mitigation systems.

In addition, some data brokers sell scores that indicate the level of risk associated with an individual or a transaction.[15] For example, a score that indicates a high level of risk may lead a business to require consumers to go through additional steps to complete a transaction, to raise its cost to the consumer, or to block the transaction entirely.[16] Some scores may correlate closely with ethnicity or financial status. For example, "aggregated" credit scores average the individual credit scores from five to 15 households in a ZIP+4 geographical area.[17] There may be little that consumers can do to affect scores that group them with others based on some shared characteristic, such as the neighborhood in which they live. The use of such scores to make risk mitigation decisions creates the potential for ethnic or financial status to have a substantial effect on consumers. More generally, in the absence of any visibility into the use of these risk mitigation products, consumers cannot make choices to avoid being scored unfavorably if they do not know that risk scores exist and how businesses use them.

Existing laws do not sufficiently address data brokers' handling of sensitive data in marketing or risk mitigation contexts. The products examined in the report do not trigger legal

---

[12] *Id.* at 32 & n.65 (discussing banks' use of identity verification products to meet customer identification requirements under the USA PATRIOT Act).
[13] *Id.* at 33.
[14] One data broker that was part of the Commission's study allows consumers to have some access to information used in its risk mitigation products. *See* DATA BROKER REPORT, *supra* note 1, at 53. In addition, the members of the credit reporting industry have long met the challenge of allowing consumers access and correction rights, and still maintained a high level of accuracy in their credit reports.
[15] *See* DATA BROKER REPORT, *supra* note 1, at 32.
[16] *See id.*
[17] In re Trans Union, Opinion of the Commission, at 12, Mar. 2000, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2000/03/transunionopinionofthecommission.pdf; *see also* Comments of Pam Dixon, Final Transcript of FTC Spring Privacy Series: Alternative Scoring Products, at 54-55, Mar. 19, 2014 (stating that "[a]ggregate credit scores apply to a neighborhood" and "I can't purchase my aggregate credit score, . . . [i]t's not regulated."), *available at* http://www.ftc.gov/system/files/documents/public_events/182261/alternative-scoring-products_final-transcript.pdf.

requirements for data brokers, their data sources, or the companies that use their products to provide access to this data or ensure its accuracy. Though the report makes clear that applying a risk mitigation label to a consumer data product or service does not, on its own, render the Fair Credit Reporting Act (FCRA) inapplicable, [18] it identifies some risk mitigation products that do not fall under the FCRA. For example, the use of a risk mitigation product by a mobile phone service provider to confirm the identity of an account applicant or to confirm that her SSN is not associated with fraud is probably not covered by the FCRA.[19] The carrier might refuse to open an account if the product reflects a risk of fraud, even if the underlying information is inaccurate. And, given the lack of transparency into these practices, it would be very hard to detect whether a risk mitigation score is being used in a manner that triggers FCRA requirements. More troubling still, some of the laws that prohibit discrimination on the basis of race and certain other categories are limited to certain settings, such as the extension of credit, and do not include marketing and risk mitigation. Thus, existing anti-discrimination laws may leave significant gaps where risk mitigation products are concerned.

To close these gaps, I urge Congress to consider legislation provisions – in addition to the provisions recommended by the Commission – that would create greater accountability for data suppliers, data brokers, and data broker clients. Creating appropriate levels of accountability requires addressing data flows both "upstream" (from data suppliers to data brokers) and "downstream" (from data brokers to users of their products). First, Congress should consider legislation – and not merely a best practice recommendation – that would require data brokers to employ reasonable procedures to ensure that their clients do not use their products for unlawful purposes.[20] Reasonable procedures could include requirements for data brokers to verify the identity of their customers, and conduct due diligence and other monitoring, to provide a level of accountability that their customers are not using data for unlawful purposes.

Data brokers are well-situated to monitor their clients' data use and to be part of an early warning system when their highly sensitive information is used for unlawful purposes. Data brokers interface directly with their clients, and can assess their clients' ability to comply with existing prohibitions on discrimination. Requiring the data brokers to monitor their clients use will create a system whereby consumers are not required to bear the entire burden of managing all privacy risk associated with data brokers' profiles,[21] and will allow those who are best situated to spot problems to help prevent consumer harms that would otherwise be difficult if not impossible to detect.

A second accountability measure that Congress should consider is to require data brokers to take reasonable steps to ensure that their original sources of information obtained appropriate consent from consumers.[22] This requirement would help to ensure that data brokers' sources comply with the Commission's recommendation that the sources secure well-informed consumer consent to disclose information to data brokers. Placing requirements on both the sources to

---

[18] *See, e.g.*, DATA BROKER REPORT, *supra* note 1, at 52-53.
[19] *See id.* at 37, 52-53.
[20] *See id.* at 56 n.108.
[21] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).
[22] *See* DATA BROKER REPORT, *supra* note 1, at 52 n.91. One example of a reasonable step that data brokers could take to ensure that their sources obtained appropriate consent from consumers is to inspect their sources' notices and choice mechanisms.

secure this consent as well as the data brokers to ensure that their sources secure this consent is a "belts and suspenders" approach that is entirely appropriate, because sources often share with data brokers information about consumers, including sensitive information, outside the context in which consumers provide the information.

*****

The data broker enterprise is complex, and involves multiple players collecting, sharing, aggregating, creating and using consumer profiles that can contain sensitive information. As the Commission has found, these profiles can be used in contexts that can adversely impact consumers. Greater transparency and accountability must be infused into this enterprise. The Commission's legislative recommendations, along with the additional recommendations that I have outlined here, would go a long way to shining a much needed light on the practices of data brokers, and to providing consumers and other interested stakeholders with meaningful tools to ensure that the narratives data brokers tell about us are accurate fair, and used in appropriate ways. I am committed to working with Congress, my colleagues at the Commission, the Administration, and other policymakers to help make these important legislative recommendations a reality.

*****

The Commission's report is the result of diligent and painstaking work by Commission staff. I applaud their efforts. I look forward to working with my colleagues at the Commission and with staff as we explore in depth other aspects of commercial use of big data, including alternative scoring products,[23] user-generated and user-controlled health data,[24] and low income and underserved consumers.[25]

[23] *See Spring Privacy Series: Alternative Scoring Products*, FED. TRADE COMM'N (Mar. 19, 2014), *available at* http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.
[24] *Spring Privacy Series: Consumer Generated and Controlled Health Data*, FED. TRADE COMM'N (May 7, 2014), *available at* http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data.
[25] Press Release, Fed. Trade Comm'n, FTC to Examine Effects of Big Data on Low Income and Underserved Consumers at September Workshop (Apr. 11, 2014) ,*available at* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-examine-effects-big-data-low-income-underserved-consumers.