DATA BROKERS

A Call for Transparency and Accountability

Federal Trade Commission
May 2014

Data Brokers

A Call for Transparency and Accountability

May 2014

Federal Trade Commission

Edith Ramirez, Chairwoman
Julie Brill, Commissioner
Maureen K. Ohlhausen, Commissioner
Joshua D. Wright, Commissioner
Terrell McSweeny, Commissioner

TABLE OF CONTENTS

List of Exhibits

EXECUTIVE SUMMARY

In today's economy, Big Data is big business. Data brokers—companies that collect consumers' personal information and resell or share that information with others—are important participants in this Big Data economy.

In this report, the Federal Trade Commission ("FTC" or "Commission") discusses the results of an in-depth study of nine data brokers. These data brokers collect personal information about consumers from a wide range of sources and provide it for a variety of purposes, including verifying an individual's identity, marketing products, and detecting fraud. Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage. By reporting on the data collection and use practices of these nine data brokers, which represent a cross-section of the industry, this report attempts to shed light on the data broker industry and its practices.

For decades, policymakers have expressed concerns about the lack of transparency of companies that buy and sell consumer data without direct consumer interaction. Indeed, the lack of transparency among companies providing consumer data for credit and other eligibility determinations led to the adoption of the Fair Credit Reporting Act ("FCRA"), a statute the Commission has enforced since its enactment in 1970. The FCRA covers the provision of consumer data by consumer reporting agencies where it is used or expected to be used for decisions about credit, employment, insurance, housing, and similar eligibility determinations; it generally does not cover the sale of consumer data for marketing and other purposes. While the Commission has vigorously enforced the FCRA,[1] since the late 1990s it has also been active in examining the practices of data brokers that fall outside the FCRA.

Most recently, in its 2012 report Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers ("Privacy Report"),[2] the Commission specifically addressed the subject of data brokers. The Commission described three different categories of data brokers: (1) entities subject to the FCRA; (2) entities that maintain data for marketing purposes; and (3) non-FCRA covered entities that maintain data for non-marketing purposes that fall outside of the FCRA, such as to detect fraud or locate people.[3] The Commission noted that, while the FCRA addresses a number of critical transparency issues associated with companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories remain opaque. In the report, the Commission recommended

1 The Commission has brought 100 FCRA enforcement actions resulting in over $30 million in penalties. *See What Information Do Data Brokers Have on Consumers, and How Do They Use It? Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. (2013) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Comm'n), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf.

2 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

3 *Id.* at 65.

legislation in this area to improve the transparency of industry practices.[4] Following the Privacy Report, the Commission determined that, despite some progress, too little was still known about the practices of data brokers and that further examination was needed.

To further the objective of increased transparency, in December 2012, the Commission initiated a study of data broker practices. It issued identical Orders to File Special Reports ("Orders") under section 6(b) of the Federal Trade Commission Act[5] to nine data brokers seeking information about their data collection and use practices, as well as any tools provided to consumers to control these practices. *Appendix A* is a copy of the text of the Orders that the Commission issued to the data brokers. The nine data brokers that received the Orders are Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future. The Orders requested detailed information regarding the data brokers' practices, including the nature and sources of consumer data they collect; how they use, maintain, and disseminate the data; and the extent to which the data brokers allow consumers to access and correct data about them or to opt out of having their personal information sold or shared.

This report summarizes the information provided in response to the Commission's Orders, including information gathered through follow-up questions and meetings and publicly available sources. In general, the data brokers collect information about consumers from a wide variety of commercial, government, and other publicly available sources. In developing their products, the data brokers use not only the raw data they obtain from these sources, such as a person's name, address, home ownership status, or age, but also certain derived data, which they infer about consumers. For example, a data broker might infer that an individual with a boating license has an interest in boating, that a consumer has a technology interest based on the purchase of a "Wired" magazine subscription, or that a consumer who has bought two Ford cars has loyalty to that brand. The data brokers use this actual and derived data to create three main kinds of products for clients in a wide variety of industries: marketing products, risk mitigation products, and people search products.

Marketing Products

Five of the data brokers studied sell marketing products, which assist clients in a variety of ways. For example, businesses can purchase their customers' email addresses from data brokers so that they can send email solicitations to them. They can also purchase information about their customers' interests in order to market specific products to them, including using consumers' offline activities to determine what advertisements to serve them on the Internet. The data brokers also sell analytics products. For instance, some data brokers analyze their client's customer data and suggest the media channel to use to advertise a particular product (e.g., online or newspapers) and/or the geographic region where the advertisements

4 *Id.* at 69.

5 15 U.S.C. § 46(b). *See also Appendix A.*

should be shown. A few data brokers also convert their analyses into marketing scores that, for example, rank clients' customers on the basis of how likely they are to respond to particular marketing efforts or to make a purchase, their presence on the web or their influence over others, or other metrics.

Most of the data brokers that sell marketing products provide consumers with limited access to some, but not all, of the actual and derived data the data brokers have about them. Only two of the data brokers allow consumers to correct their personal information for marketing purposes, and four of the five data brokers that sell marketing products allow consumers to opt out of the use of their personal information for marketing purposes. However, it is not clear how consumers would learn about these rights; for example, no centralized portal currently exists for consumers to learn about data brokers and what access rights and choices they provide.

Risk Mitigation Products

Four of the data brokers studied sell risk mitigation products, which clients use to verify their customers' identities or detect fraud. For example, a lender might use a data broker's identity verification product to ensure that the individual presenting himself as John Smith at 123 Main Street who wants to open an account is in fact that John Smith. The same lender might use a fraud detection product to flag whether a Social Security number provided as part of the application process has recently been associated with many different addresses, thereby suggesting fraud.

Even if consumers knew about the data brokers providing products in this category or knew they were denied or limited in their ability to complete a transaction, they might not be able to access their own information from these data brokers and correct errors. Two of the data brokers studied provide consumers with some form of access to their information used in risk mitigation products after verifying their identity, but only one allows consumers to correct their information.

People Search Products

Three of the data brokers studied provide "people search" websites through which users can search for publicly available information about consumers. Users can use these products to research corporate executives and competitors, find old friends, look up a potential love interest or neighbor, network, or obtain court records or other information about consumers. Consumers can generally access their information through the same free or fee-based products that the data brokers provide to their clients. These data brokers allow consumers to correct certain information to varying degrees; most of them also allow consumers to opt out of the disclosure of their information.

Based on the information obtained, the Commission makes the following findings.

Findings

1. Characteristics of the Industry

- **Data Brokers Collect Consumer Data from Numerous Sources, Largely Without Consumers' Knowledge**: Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

- **The Data Broker Industry is Complex, with Multiple Layers of Data Brokers Providing Data to Each Other**: Data brokers provide data not only to end-users, but also to other data brokers. The nine data brokers studied obtain most of their data from other data brokers rather than directly from an original source. Some of those data brokers may in turn have obtained the information from other data brokers. Seven of the nine data brokers in the Commission's study provide data to each other. Accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers.

- **Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer**: Data brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction. Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases. Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer.

- **Data Brokers Combine and Analyze Data About Consumers to Make Inferences About Them, Including Potentially Sensitive Inferences:** Data brokers infer consumer interests from the data that they collect. They use those interests, along with other information, to place consumers in categories. Some categories may seem innocuous such as "Dog Owner," "Winter Activity Enthusiast," or "Mail Order Responder." Potentially sensitive categories include those

that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African Americans with low incomes. Other potentially sensitive categories highlight a consumer's age such as "Rural Everlasting," which includes single men and women over the age of 66 with "low educational attainment and low net worths," while "Married Sophisticates" includes thirty-something couples in the "upper-middle class . . . with no children." Yet other potentially sensitive categories highlight certain health-related topics or conditions, such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus."

- **Data Brokers Combine Online and Offline Data to Market to Consumers Online:** Data brokers rely on websites with registration features and cookies to find consumers online and target Internet advertisements to them based on their offline activities. Once a data broker locates a consumer online and places a cookie on the consumer's browser, the data broker's client can advertise to that consumer across the Internet for as long as the cookie stays on the consumer's browser. Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities. Some data brokers are using similar technology to serve targeted advertisements to consumers on mobile devices.

2. Benefits and Risks

- **Consumers Benefit from Many of the Purposes for Which Data Brokers Collect and Use Data**: Data broker products help to prevent fraud, improve product offerings, and deliver tailored advertisements to consumers. Risk mitigation products provide significant benefits to consumers by, for example, helping prevent fraudsters from impersonating unsuspecting consumers. Marketing products benefit consumers by allowing them to more easily find and enjoy the goods and services they need and prefer. In addition, consumers benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers they may not have otherwise been able to reach. Similarly, people search products allow individuals to connect with old classmates, neighbors, and friends.

- **At the Same Time, Many of the Purposes for Which Data Brokers Collect and Use Data Pose Risks to Consumers**: There are a number of potential risks to consumers from data brokers' collection and use of consumer data. For example, if a consumer is denied the ability to conclude a transaction based on an error in a risk mitigation product, the consumer can be harmed without knowing why. In such cases, the consumer is not only denied the immediate benefit, but also cannot take steps to prevent the problem from recurring. Similarly, the scoring processes used in some marketing products are not transparent to consumers. This

means that consumers are unable to take actions that might mitigate the negative effects of lower scores, such as being limited to ads for subprime credit or receiving different levels of service from companies. As to other marketing products, they may facilitate the sending of advertisements about health, ethnicity, or financial products, which some consumers may find troubling and which could undermine their trust in the marketplace. Moreover, marketers could even use the seemingly innocuous inferences about consumers in ways that raise concerns. For example, while a data broker could infer that a consumer belongs in a data segment for "Biker Enthusiasts," which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using that same segment might infer that the consumer engages in risky behavior. Similarly, while data brokers have a data category for "Diabetes Interest" that a manufacturer of sugar-free products could use to offer product discounts, an insurance company could use that same category to classify a consumer as higher risk. Finally, people search products can be used to facilitate harassment, or even stalking, and may expose domestic violence victims, law enforcement officers, prosecutors, public officials, or other individuals to retaliation or other harm.

- **Storing Data About Consumers Indefinitely May Create Security Risks**: Some of the data brokers store all data indefinitely, even if it is later updated, unless otherwise prohibited by contract. For some products, these data brokers report that they need to keep older data. For example, they explain that even if a consumer's address is outdated, it is important to keep the consumer's address history in order to verify the consumer's identity. For other products, however, retention of older data may not be necessary. An older address may be less relevant to deliver marketing to a consumer. Although stored data may be useful for future business purposes, the risk of keeping the data may outweigh the benefits. For example, identity thieves and other unscrupulous actors may be attracted to the collection of consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials.

3. Consumer Choice

- **To the Extent Data Brokers Offer Consumers Choices About Their Data, the Choices are Largely Invisible and Incomplete**: Some data brokers provide consumers with choices about their data, but because data brokers are not consumer-facing, consumers may not know where to go to exercise any choices that may be offered. In addition, the data brokers' opt outs do not clearly convey whether the consumer can exercise a choice to opt out of all uses of consumer data, and therefore, consumers may find the opt outs confusing. As a result, even those consumers who know who the data brokers are, find their websites, and take the time to find the opt out and use it may still not know its limitations. For marketing products,

the extent of consumers' choices over their data is not clear. For risk mitigation products, many data brokers do not provide consumers with access to their data or the ability to correct inaccurate data.

Many of these findings point to a fundamental lack of transparency about data broker industry practices. Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge.

In light of these findings, the Commission unanimously renews its call for Congress to consider enacting legislation that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities. The specific legislative recommendations made by the Commission reflect high-level principles drawn from the findings of this study, the Commission's previous work in this area, and the ongoing public debate about data brokers.[6] In particular, the recommendations build on the Commission's work for the last two decades to improve transparency and choice in the data broker industry. Indeed, despite the Commission's call for greater transparency in the 1990s, the Individual References Services Group ("IRSG") self-regulatory experiment to improve transparency of data broker practices was short-lived.[7] Since then, data broker practices have grown dramatically, in both breadth and depth, as data brokers have expanded their ability to collect information from a greater number of sources, including from consumers' online activities; analyze it through new algorithms and emerging business models; and store the information indefinitely due to reduced storage costs. Despite the Commission's past recommendations, lack of transparency and choice remain a significant source of concern about this industry.

The Commission's legislative recommendations vary depending on the product categories at issue—marketing, risk mitigation, or people search—and reflect differences in the business models and the

6 The legislative and best practice recommendations, both in the Executive Summary and in Findings and Recommendations, Section VIII of the Report, reflect the consensus of a majority of the Commission. To the extent that particular Commissioners have different viewpoints on a particular legislative or best practice recommendation, those viewpoints can be found in footnotes in the Findings and Recommendations, Section VIII of the Report, or in a separate statement. Commissioner McSweeny did not participate in the Commission vote on this report.

7 *See* Fed. Trade Comm'n, Individual Reference Services, A Report to Congress (1997), *available at* http://www.ftc.gov/reports/individual-reference-services-report-congress. In September 2001, approximately four years after it was established, the IRSG announced its termination. *See Notice of Termination of IRSG*, IRSG, http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm (last visited May 19, 2014) (accessed by searching the Internet Archive index and viewing the Dec. 8, 2002, version of this page).

sensitivity of the data used. Many of these legislative recommendations are consistent with best practices that certain of the nine data brokers have already implemented.[8]

Legislative Recommendations

With respect to data brokers that sell marketing products, the Commission recommends that Congress consider legislation requiring data brokers to provide consumers access to their data, including sensitive data held about them, at a reasonable level of detail, and the ability to opt out of having it shared for marketing purposes. The Commission recommends that Congress consider including four requirements in any such legislation. First, Congress should seek to enable consumers to easily identify which data brokers may have data about them and where they should go to access such information and exercise opt-out rights. Legislation could 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. Second, Congress should consider requiring data brokers to clearly disclose to consumers (e.g., on their websites) that they not only use the raw data that they obtain from their sources, such as a person's name, address, age, and income range, but that they also derive from the data certain data elements. Allowing consumers to access data about themselves is particularly important in the case of sensitive information—and inferences about sensitive consumer preferences and characteristics—such as those relating to certain health information. Third, Congress should consider requiring data brokers to disclose the names and/or categories of their sources of data, so that consumers are better able to determine if, for example, they need to correct their data with an original public record source. Finally, Congress should consider requiring consumer-facing entities to provide a prominent notice to consumers that they share consumer data with data brokers and provide consumers with choices about the use of their data, such as the ability to opt-out of sharing their information with data brokers. Congress should also consider protecting sensitive information, such as certain health information, by requiring that consumer-facing sources obtain consumers' affirmative express consent before they collect sensitive information. Because few consumers know about the existence of data brokers, meaningful notice from the data source provides an important opportunity for consumers to learn that their data is shared with data brokers and how to exercise control over the use of their data.

For data brokers that sell risk mitigation products, the Commission recommends that Congress consider legislation that provides consumers with transparency when a company uses a risk mitigation product to limit consumers' ability to complete a transaction. Specifically, when a risk mitigation product adversely impacts a consumer's ability to obtain certain benefits, the consumer-facing company should identify the

8 For example, since the Commission began its study, Acxiom, one of the data brokers at issue in this report, has publicly announced changes to its access policy and launched a new website that allows consumers to access, correct, and opt out of having information about themselves included in certain marketing products. *See* Press Release, Acxiom Corp., Acxiom Launches New Consumer Portal (Sept. 4, 2013), *available at* http://www.acxiom.com/acxiom-launches-new-consumer-portal/.

data brokers whose data the company relied upon; these data brokers could, in turn, give consumers the right to access the information used and, where appropriate, correct any erroneous information. The level of transparency, access, and correction should be tied to the significance of the benefit or transaction in question. At the same time, the Commission recognizes that it may be appropriate for legislation to require data brokers to implement robust authentication safeguards before allowing such access and correction so that an unscrupulous individual cannot "correct" accurate data. Congress should consider how to enable consumer access while preserving the accuracy and security of such data.

The Commission also recommends Congress consider legislation that would require data brokers offering people search products to: (1) allow consumers to access their own information; (2) allow consumers to suppress the use of this information;[9] (3) disclose to consumers the data brokers' sources of information, so that, if possible, consumers can correct their information at the source; and (4) disclose any limitations of the opt-out option, such as the fact that close matches of an individual's name may continue to appear in search results.

Best Practice Recommendations

More generally, the Commission calls on the data broker industry to adopt several best practices. First, they should implement privacy-by-design, which includes considering privacy issues at every stage of product development. Second, the Commission encourages data brokers to implement better measures to refrain from collecting information from children and teens, particularly in marketing products. Finally, the Commission recommends that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes.

9 The data brokers use the term "suppress" to indicate that, although certain data may appear in their databases, they prevent the data from being included in their products.

I. INTRODUCTION

A. Background

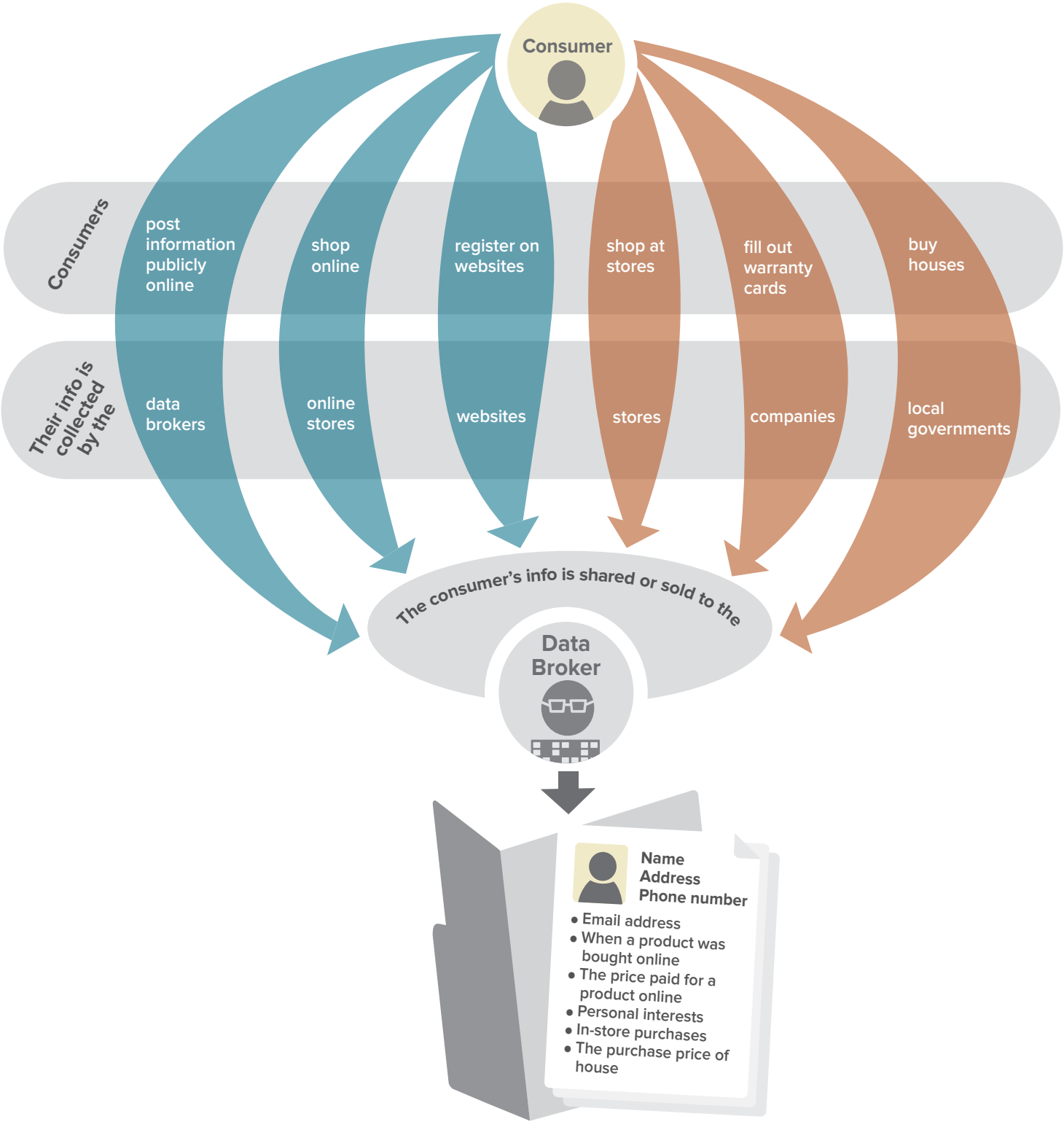
On a daily basis, consumers engage in a variety of online and offline activities that reveal personal information about them. Some typical activities include using a mobile device, shopping for a home or car, subscribing to a magazine, making a purchase at a store or through a catalog, browsing the Internet, responding to a survey in order to get a coupon, using social media, subscribing to online news sites, or entering a sweepstakes. As consumers engage in these daily activities, the entities they interact with collect information about them and, in many instances, provide or sell that information to data brokers.[1]

1 *See, e.g.*, *Sharing Information: A Day in Your Life*, Fed. Trade Comm'n, http://www.consumer.ftc.gov/media/video-0022-sharing-information-day-your-life (last visited May 19, 2014).

Exhibit 1:

Data Collection
Online & Offline

As consumers go about their business, data brokers may collect information about them.



This report examines and makes findings and recommendations with respect to the practices of data brokers—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. Significantly, data brokers typically collect, maintain, manipulate, and share a wide variety of information about consumers without interacting directly with them. Indeed, as discussed further below, data brokers collect data from a variety of sources, ranging from criminal records to property data to purchase history to warranty card registration information. In addition to using raw data, data brokers often aggregate and analyze it to make inferences about specific consumers. For example, they may categorize a consumer as an expectant parent, a car enthusiast, interested in diabetes, a discount shopper, and more likely to be interested in brand medications than generic. Other data brokers may flag a consumer's Social Security number ("SSN") as potentially associated with fraud.

Data brokers provide the information they compile to clients, who can use it to benefit consumers. Their clients may use the information to send relevant offers and coupons to consumers, which can give consumers more choices and lower their costs for searching for products and services. In addition, consumers may benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers that they may not have otherwise been able to reach. Data broker clients can also use data broker products to detect and prevent fraud, which can lower costs for businesses and, in turn, consumers.

At the same time, data broker practices may raise privacy concerns. Data brokers typically collect, manipulate, and share information about consumers without interacting directly with them. Consumers are largely unaware that data brokers are engaging in these practices and, to the extent that data brokers offer consumers explanations and choices about how the data brokers use their data, that information may be difficult to find and understand.

This report reflects the record developed through the Federal Trade Commission's ("Commission" or "FTC") issuance of Orders to File Special Reports ("Orders") to nine data brokers pursuant to Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. § 46(b). The Orders sought information about the data brokers' practices starting January 1, 2010, related to the collection and use of consumer data. This report also reflects information gathered through follow-up communications and meetings and from publicly available sources.

B. The Commission's Past Efforts to Improve Transparency of Data Broker Practices

For decades, policymakers have expressed concerns about the transparency of companies that buy and sell consumer data. Indeed, the existence of companies selling consumer data for credit and other eligibility determinations with little consumer awareness or transparency led to the enactment in 1970 of the Fair Credit Reporting Act ("FCRA"),[2] a statute the Commission has since enforced. The FCRA primarily regulates consumer reporting agencies ("CRAs"), which compile consumers' information and provide it to companies making credit, employment, insurance, housing, and similar decisions. Among other things, the FCRA requires CRAs to undertake reasonable procedures to ensure the maximum possible accuracy of consumer information they provide; it also requires CRAs to provide consumers with the right to access and correct their consumer reports.

In addition to enforcing the FCRA, the Commission has hosted workshops, drafted reports, and testified before Congress about the privacy implications of data brokers' practices.[3] In 1997, the Commission held a workshop to examine database services used to locate, identify, or verify the identity of individuals, referred to at the time as "individual reference services." The workshop prompted industry members to form the self-regulatory Individual References Services Group ("IRSG"). The Commission subsequently issued a report on the workshop and the IRSG in which it commended the IRSG for its self-regulatory efforts, but noted that its principles did not do enough to address the lack of transparency of data broker practices.[4] After

2 15 U.S.C. §§ 1681–1681x (2012).

3 *See, e.g.*, *What Information Do Data Brokers Have on Consumers, and How Do They Use It? Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. (2013) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Comm'n) [hereinafter *FTC Statement on Data Brokers*], *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf; *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information Before the S. Comm. on Banking, Hous., & Urban Affairs*, 109th Cong. (2005) (statement of Deborah Majoras, Chairman, Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf; *The Information Marketplace: Merging and Exchanging Consumer Data*, Fed. Trade Comm'n (Mar. 13, 2001), http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml. *See also* Press Release, Fed. Trade Comm'n, Information Flows: The Costs and Benefits Related to the Collection and Use of Consumer Information (June 18, 2003), *available at* http://www.ftc.gov/news-events/press-releases/2003/06/information-flows-costs-and-benefits-consumers-and-businesses.

4 *See* Fed. Trade Comm'n, Individual Reference Services, A Report to Congress (1997), *available at* http://www.ftc.gov/reports/individual-reference-services-report-congress.

industry terminated the IRSG in September 2001,[5] a series of public breaches—including several involving ChoicePoint—ultimately led to renewed scrutiny of the practices of data brokers.[6]

In recent years, the development of new technologies and business models, such as social media and mobile applications, has dramatically increased the availability, variety, and volume of consumer data.[7] New forms of tracking and increasingly powerful analytics capabilities have emerged, such as mobile tracking and analytics services that enable tracking of users across devices so that companies can communicate a timely message tailored to a consumer based on the consumer's location.[8] With these new sources and technologies, along with competitive demands from companies to seek more data about more consumers on an increasingly granular level, data brokers are finding new opportunities to collect, compile, package, and sell the consumer information they obtain.

In its 2012 report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers ("Privacy Report"),[9] the Commission discussed the privacy concerns raised by the practices of data brokers and identified three different categories of data brokers: (1) entities subject to the FCRA; (2) entities that maintain data for marketing purposes;[10] and (3) entities that maintain data for non-marketing purposes that fall outside of the FCRA, such as to detect fraud or locate people. In the Privacy Report, the Commission noted that, while the FCRA addresses a number of critical transparency issues associated with companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories operate largely in the dark.

The Commission's Privacy Report made two primary recommendations to improve the transparency of the practices of data brokers, which built on the prior work of the agency. First, the Commission renewed

5 In September 2001, approximately four years after it was established, the IRSG announced its termination. *See Notice of Termination of IRSG*, IRSG, http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm (last visited May 19, 2014) (accessed by searching the Internet Archive index and viewing the Dec. 8, 2002, version of this page).

6 *See, e.g.*, Complaint at 4, Reed Elsevier Inc., No. C-4226 (F.T.C. July 29, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf; Complaint at 4–7, United States v. ChoicePoint, No. 1:06-CV-0198-JTC (N.D. Ga. Feb. 16, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf. *See also* Press Release, Fed. Trade Comm'n, Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months (Oct. 19, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers.

7 *See* U.S. Gov't Accountability Office, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace (2013), *available at* http://www.gao.gov/products/GAO-13-663.

8 On February 19, 2014, the FTC hosted a seminar on Mobile Device Tracking, as part of a series of seminars to examine the privacy implications of new areas of technology. *See Spring Privacy Series: Mobile Device Tracking*, Fed. Trade Comm'n (Feb. 19, 2014), http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

9 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter Privacy Report]. Commissioner Ohlhausen and Commissioner Wright were not members of the Commission at that time and thus did not participate in the vote on the report.

10 The FCRA covers consumer report information used to make eligibility determinations in connection with credit, insurance, and employment. It generally does not cover information used for marketing purposes.

a call for legislation that it had first recommended in 2009,[11] which would have provided consumers with access to information data brokers held about them, in order to improve the transparency of the industry's practices. In its recommendations, the Commission emphasized that the level of access should be reasonable in light of the privacy issues raised, meaning that it should be in proportion to the nature, sensitivity, and use of the data. Subsequently, in testimony before Congress, the Commission reaffirmed its support for legislation that would provide consumers with such reasonable access.[12]

Second, the Commission recommended best practices to improve the transparency of the data broker industry. For example, it proposed exploring the idea of a centralized website where data brokers that compile and sell data for marketing purposes could identify themselves to consumers, describe how they collect consumer information, disclose the types of companies to which they sell the information, and explain the access rights and other choices they offer consumers.[13] The Commission's recommendations regarding data brokers built on almost two decades of work on these issues[14]—indeed, decades marked by an expansion in the number of data brokers and the richness of data they collect, but little progress in providing transparency and choices to consumers about their practices. While the Commission recognizes the benefits that data brokers offer, it continues to support legislation to provide consumers with more information and meaningful choices about data broker practices.

The Commission is not alone in calling for greater transparency of the data broker industry. In September 2013, the U.S. Government Accountability Office released a report on the practices of data

11 *See Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act Before the H.R. Comm. on Energy & Commerce*, 111th Cong. (2009) (statement of Eileen Harrington, Acting Director of the Bureau of Consumer Protection, Fed. Trade Comm'n), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-legislative-hearing-h.r.2221-data-accountability-and-protection-act-and-h.r.1319-informed-p2p-user-act/p064504peertopeertestimony.pdf.

12 *See The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. on Commerce, Sci., & Transp.*, 112th Cong. (2012) (statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/testimony/120509privacyprotections.pdf.

13 Privacy Report, *supra* note 9, at 69–70. The current website of the Direct Marketing Association offers choices to consumers to opt out of receiving direct marketing materials, such as catalogs. This could be a potential model for such a website. *See* DMAChoice, https://www.dmachoice.org/ (last visited May 19, 2014).

14 The Commission's two decades of work regarding the data broker industry began when the Commission held its first public workshop on Internet privacy in April 1995. In a series of hearings held in October and November 1995, the FTC examined the implications of globalization and technological innovation for competition and consumer protection issues, including privacy concerns. This workshop culminated in an FTC Staff Report. Fed. Trade Comm'n, Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace (1996), *available at* http://www.ftc.gov/reports/anticipating-21st-century-competition-consumer-protection-policy-new-high-tech-global. Expanding on this work, at a public workshop in June 1996, the Commission examined a wide range of consumer privacy issues, including website practices with respect to the collection and use of consumers' personal information. FTC staff issued a report summarizing this workshop. Fed. Trade Comm'n, Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure (Dec. 1996), *available at* http://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure. Finally, in June 1997, the agency held a four-day workshop to explore issues relating to unsolicited commercial e-mail, online privacy, children's online privacy, and individual reference services. Press Release, Fed. Trade Comm'n, FTC Privacy Week—June 10–13 (June 4, 1997), *available at* http://www.ftc.gov/news-events/press-releases/1997/06/ftc-privacy-week-june-10-13.

brokers and concluded that Congress should consider legislation to reflect the challenges posed by changes in technology, the increased market for consumer information, and the lack of transparency of the data broker industry.[15] Congress has also investigated data broker activities. In December 2013, the U.S. Senate Committee on Commerce, Science and Transportation released a Majority Staff report summarizing its investigation into how data brokers collect, compile, and sell consumer information.[16] The report concluded that data brokers that sell data for marketing purposes operate with minimal transparency and are subject to virtually no statutory consumer protections.[17] And on February 12, 2014, Senators Jay Rockefeller and Ed Markey introduced a bill, entitled "Data Broker Accountability and Transparency Act," that would improve transparency of data broker practices by, among other things, requiring data brokers to make available the information they have collected about each consumer.[18] Similarly, U.S. Representatives Bobby L. Rush and Joe Barton re-introduced a bipartisan bill, entitled "The Data Accountability and Trust Act of 2014," that would improve transparency of data broker practices by, among other things, requiring data brokers to make available at least once per year the information they have collected about each consumer.[19]

C. Data Broker Study

To further the objective of increased transparency, in December 2012, the Commission initiated a study of data broker practices. It issued identical Orders to nine data brokers seeking information about the recipients' information collection and use practices. The Orders contained requests for information and documents about each data broker's products and services, data collection practices, the sources of its data, its clients, and the extent to which it provides consumers with access to and control of their information. *Appendix A* is a copy of the text of the Orders that the Commission issued to the data brokers.

The Commission did not seek information about the data brokers' activities that fall within the scope of the FCRA.[20] As noted above, the FCRA generally governs the practices of entities that assemble or evaluate consumer information for use by creditors, employers, insurance companies, landlords, and others

15 *See* U.S. Gov't Accountability Office, *supra* note 7, at 46. In its report, the GAO analyzed laws, studies, and other documents, and interviewed representatives of federal agencies, the data broker industry, consumer and privacy groups, and others. The report contains an extensive discussion of existing laws affecting the data broker industry.

16 Majority Staff of S. Comm. on Commerce, Sci., & Transp., Office of Oversight & Investigations, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (2013) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577. The Committee found that data brokers collect and maintain data on hundreds of millions of consumers, which they analyze, package, and sell for a variety of purposes.

17 *Id.* In addition, on July 24, 2012, eight members of the House of Representatives sent a letter to nine data brokers asking for information about how the companies amass, refine, sell, and share consumer data. *See* Natasha Singer, *Congress to Examine Data Sellers*, N.Y. Times (July 24, 2012), http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html?_r=0.

18 *See* Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014).

19 The Data Accountability and Trust Act of 2014, H.R. 4400, 113th Cong. (2014).

20 Some of the data brokers studied sell FCRA and non-FCRA covered products.

engaged in making certain eligibility determinations affecting consumers. It allows consumers to access their consumer reports and dispute inaccurate information about them.

The nine data brokers that received the Orders are as follows:

1. **Acxiom:** Acxiom provides consumer data and analytics for marketing campaigns and fraud detection. Its databases contain information about 700 million consumers worldwide with over 3000 data segments for nearly every U.S. consumer.[21]

2. **Corelogic:** Corelogic provides data and analytic services to businesses and government based primarily on property information, as well as consumer and financial information. Its databases include over 795 million historical property transactions, over ninety-three million mortgage applications, and property-specific data covering over ninety-nine percent of U.S. residential properties, in total exceeding 147 million records.[22]

3. **Datalogix:** Datalogix provides businesses with marketing data on almost every U.S. household and more than one trillion dollars in consumer transactions.[23] In September 2012, Facebook announced a partnership with Datalogix to measure how often Facebook's one billion users see a product advertised on the social site and then complete the purchase in a brick and mortar retail store.[24]

4. **eBureau:** eBureau provides predictive scoring and analytics services for marketers, financial services companies, online retailers, and others. eBureau primarily offers products that predict whether someone is likely to become a profitable customer or whether a transaction is likely to conclude in fraud. It provides clients with information drawn from billions of consumer records,[25] adding over three billion new records each month.[26]

5. **ID Analytics:** ID Analytics provides analytics services designed principally to verify people's identities or to determine whether a transaction is likely fraudulent. The ID Analytics network

21 Acxiom Corp., Annual Report 8 (2013), *available at* http://d3u9yejw7h244g.cloudfront.net/wp-content/uploads/2013/09/2013-Annual-Report.pdf.

22 Corelogic, Annual Report 7 (2012), *available at* http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MTkwNDg0fENoaWxkSUQ9LTF8VHlwZT0z&t=1.

23 *About Us*, Datalogix, http://www.datalogix.com/about/ (last visited May 19, 2014).

24 Joey Tyson, *Relevant Ads That Protect Your Privacy*, Facebook (Sept. 30, 2012, 8:55AM), https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125.

25 *Find Your Next Customer Through Predictive Analytics*, eBureau, http://www.ebureau.com/sites/default/files/file/ebureau_solutions_brochure.pdf (last visited May 19, 2014).

26 *eScores*, eBureau, http://www.ebureau.com/sites/default/files/file/datasheets/ebureau_escore_datasheet.pdf (last visited May 19, 2014).

includes hundreds of billions of aggregated data points, 1.1 billion unique identity elements, and it covers 1.4 billion consumer transactions.[27]

6. **Intelius:** Intelius provides businesses and consumers with background check and public record information. Its databases contain more than twenty billion records.[28]

7. **PeekYou:** PeekYou has patented technology that analyzes content from over sixty social media sites, news sources, homepages, and blog platforms to provide clients with detailed consumer profiles.[29]

8. **Rapleaf:**[30] Rapleaf is a data aggregator that has at least one data point associated with over eighty percent of all U.S. consumer email addresses.[31] Rapleaf supplements email lists with the email address owner's age, gender, marital status, and thirty other data points.[32]

9. **Recorded Future:** Recorded Future captures historical data on consumers and companies across the Internet and uses that information to predict the future behavior of those consumers and companies. As of May 2014, Recorded Future had access to information from over 502,591 different open Internet sites.[33]

The Commission selected these data brokers because they represent a broad swath of activity from a cross-section of large, mid-sized, and small data brokers. The Commission also considered their prominence in the industry; the amount and types of data they collect; their use of different models to find, collect, and analyze data; and the range of products they sell. While some of these data brokers are established entities, others are new entrants to the data broker market.

The data brokers submitted Special Reports in response to the Orders, responded to follow-up questions, and met with Commission staff to provide additional clarification regarding their business models and practices. The Commission used the information obtained from the data brokers and from publicly available sources to prepare this report. Consistent with Sections 6(f) and 21(d) of the FTC Act, information that the

27 *Leverage Deep Insight Into Consumer Identity Behavior*, ID Analytics, https://web.archive.org/web/20130901122631/http://www.idanalytics.com/technology/ (last visited May 19, 2014) (accessed by searching the Internet Archive index and viewing the Sept. 1, 2013 version of this page).

28 *Intelius Facts*, Intelius, http://corp.intelius.com/intelius-facts (last visited May 19, 2014).

29 *About Us*, PeekYou, http://www.peekyou.com/about/ (last visited May 19, 2014).

30 In August 2012, Rapleaf became a wholly-owned subsidiary of LiveRamp. In October 2013, TowerData purchased Rapleaf's assets and Rapleaf was dissolved. Press Release, TowerData, Inc., TowerData Acquires Rapleaf, Forges Comprehensive Email Data Solutions Company (Oct. 1, 2013), *available at* http://www.towerdata.com/company/news/towerdata-acquires-rapleaf-press-release/. In its response to the Orders, Rapleaf provided information for both Rapleaf and LiveRamp, which, for the purpose of this report, were treated as one entity. In May 2014, Acxiom acquired LiveRamp. Press Release, Acxiom Corp., Acxiom to Acquire LiveRamp (May 14, 2014), *available at* http://www.acxiom.com/acxiom-liveramp/.

31 *Fast. Simple. Secure.*, Rapleaf, http://www.rapleaf.com/why-rapleaf/ (last visited May 19, 2014).

32 *Batch Append*, Rapleaf, http://www.rapleaf.com/pricing-append/ (last visited May 19, 2014).

33 Recorded Future, https://www.recordedfuture.com/ (last visited May 19, 2014).

data brokers have designated as confidential or privileged commercial or financial information is reported on an aggregate basis, without naming the particular company to which it pertains.

This report describes several key practices staff examined through the Commission's Orders. First, it identifies how and from where the data brokers acquire their data. Second, it describes how the data brokers develop their products from this raw data. Third, it discusses the types of products the data brokers provide to their clients.[34] Fourth, it explains the data brokers' procedures to ensure the quality of their products. Fifth, it describes the assortment of clients that use the data broker products. Finally, it describes the options the data brokers give to consumers to access, suppress, and correct their own data.

34 As noted above, the Orders focused on the data brokers' non-FCRA covered products.

II. DATA ACQUISITION

A. Sources of Data

None of the nine data brokers collect data directly from consumers. Rather, they collect data from numerous other sources, which fall into three categories: (1) government sources; (2) other publicly available sources; and (3) commercial sources. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

1. Government Sources

a. Federal Government

All but three of the nine data brokers obtain information directly from federal government sources. For example, the U.S. Census Bureau provides information about the demographics of particular city blocks, such as ethnicity, age, education level, household makeup, income, occupations, and commute times. In addition, it provides geographic information including roads, addresses, congressional districts, and boundaries for cities, counties, subdivisions, and school and voting districts. The Social Security Administration provides information such as the Death Master File, which includes consumers' names, SSNs, and dates of death. The U.S. Postal Service provides information such as address standardization and change of address information. Other federal and international agencies, such as the Federal Bureau of Investigation, U.S. Secret Service, and European Union, provide information related to terrorist watch lists or most wanted lists. In addition, federal and international agencies provide lists of individuals who are ineligible to receive government contracts or other benefits.[35] Also, federal courts provide information on bankruptcies.

b. State and Local Governments

State and local governments offer a wide variety of information, including:

- Professional licenses (e.g., licenses for pilots, doctors, lawyers, architects)
- Recreational licenses (e.g., hunting and fishing licenses)
- Real property and assessor records
  - Taxes

35 For example, such lists are maintained and provided by the U.S. Office of Foreign Assets Control, U.S. Immigration and Customs Enforcement, and the U.S. Department of State.

  - Assessed Value
  - Liens
  - Deeds
  - Mortgages
  - Mortgage Releases
  - Pre-foreclosures
  - Identifying information about the owner
  - Information about the property (e.g., square footage, number of bathrooms and bedrooms, and whether the property has a pool)
- Voter registration information (e.g., name, address, date of birth, and party affiliation)
- Motor vehicle and driving records
- Court records
  - Criminal records
  - Civil actions and judgments
  - Birth, marriage, divorce, and death records

Two points are worth highlighting in connection with this information. First, some of the data brokers do not obtain this information directly from state and local governments. Rather, they obtain the information from other data brokers that either hire people to visit local offices to compile the information or that have relationships with these offices that allow them to acquire this information automatically (e.g., through an online portal). The data brokers identified nearly twenty-five other data brokers from which they obtain state and local government information.

Second, some laws restrict the use of this information. For example, at least twenty-two states prohibit the use of voter registration records for commercial or non-election-related purposes.[36] In addition, the federal Driver's Privacy Protection Act ("DPPA")[37] and some state laws contain restrictions that apply to

36 States restricting the use of such information for commercial purposes include California, Georgia, Illinois, Kansas, Maryland, Missouri, Montana, Nebraska, New Hampshire, New Jersey, Oregon, South Dakota, West Virginia, and Wyoming.

37 Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–2725 (2012).

state motor vehicle departments.[38] For instance, the DPPA prohibits the disclosure of motor vehicle and driving record information, except for limited purposes such as law enforcement, insurance, and identity verification or fraud detection. It allows the unrestricted use of such information with the express consent of the individual, which at least one state requests in its driver's license application.[39]

2. Publicly Available Sources, Including Social Media, Blogs, and the Internet

Over half of the data brokers reported that they obtain other publicly available information, including telephone and other directories, press reports, and information that individuals post on the Internet, including blogs and social media sites. For example, some of them obtain information by crawling social media sites, such as Bebo and LinkedIn, where individuals have not set their privacy settings to restrict access to their information and the social media sites have given the data brokers access to such information.[40] As with government sources, these data brokers either obtain information directly from these sources or, in limited instances, from other data brokers that compile such information.

3. Commercial Data Sources

All but one of the data brokers in this study purchase information about individuals from wide-ranging commercial sources. For example, the data brokers obtain detailed, transaction-specific data about purchases from retailers and catalog companies. Such information can include the types of purchases (e.g., high-end shoes, natural food, toothpaste, items related to disabilities or orthopedic conditions), the dollar amount of the purchase, the date of the purchase, and the type of payment used. Several of the data brokers also obtain information from magazine publishers about the types of subscriptions sold.

Three data brokers obtain customer lists from registration websites, which are sites where consumers register or log in to obtain services, such as retail, news, and travel sites. Such lists can include a consumer's name, along with a postal or email address. A few of the data brokers obtain aggregated transaction data from financial services companies. The types of data that the data brokers obtain from these sources include

38 At least twenty-three states have state laws governing the disclosure of motor vehicle records that prohibit companies from using such information, except for limited purposes such as identity verification or fraud prevention (i.e., Connecticut, Idaho, Illinois, Indiana, Kansas, Maryland, Michigan, North Dakota, Nebraska, New Hampshire, New Jersey, New Mexico, Ohio, Oklahoma, Oregon, Rhode Island, South Dakota, Tennessee, Texas, West Virginia, Colorado, Arizona, and Alaska). Other states prohibit access to this information in virtually all circumstances (i.e., Montana, Washington, and Delaware).

39 *Driver License/Identification Card Application*, Ariz. Dep't of Transp., *available at* http://www.azdot.gov/docs/default-source/mvd-forms-pubs/40-5122.pdf?sfvrsn=11 (last visited May 19, 2014).

40 According to the data brokers, some social media sites restrict third parties' ability to collect data from their sites in an automated way. For example, some of the data brokers stated that Facebook only allows specified search engines to crawl its site, and its Terms of Service bar scraping, or the copying of the information on Facebook's website, without Facebook's written permission. The Commission did not independently examine the policies of social media sites as part of this study.

more sensitive information (e.g., certain health-related purchases[41]) and less sensitive information (e.g., certain clothing purchases).

Some of the data brokers report that they obtain data directly from their merchant and financial service company clients, either to create or enhance products or services for those particular clients or to use in other products in aggregated, de-identified form, as explained further below. Other data, such as some data from registration websites, comes from non-client consumer-facing companies pursuant to specific contractual arrangements. At least one of the nine data brokers obtains consumers' web browsing activities from online advertising networks.

Most of the commercially sourced data, however, comes from other data brokers outside this study. For example, the data brokers in this study obtain information from other data brokers that:

- Obtain information from telephone companies about consumers who have recently created a new landline account;
- Obtain information from automobile dealers about sales and service, warranty, and aftermarket repairs;
- Aggregate and model the purchase history of 190 million individual consumers from more than 2600 merchants; and
- Compile self-reported information that consumers provide online or offline through marketing surveys, warranty registrations, and contests. One data broker that compiles self-reported information maintains data of over 240 million consumers sorted into 1000 interest categories.

Several of the data brokers share the same sources. And each data broker utilizes multiple sources for similar data. For example, one of the data brokers in this study obtains consumers' contact information from twenty different sources.[42]

In addition, seven of the nine data brokers buy from or sell information to each other. Accordingly, it may be virtually impossible for a consumer to determine the originator of a particular data element. As shown in Exhibit 2, which depicts the flow of data among the nine data brokers in this study, the consumer would have to retrace the path of data through a series of data brokers to finally arrive at the original source.

41 The health-related purchases are not covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which protects the privacy of certain health-related information. The data brokers are not covered entities under HIPAA, which are defined to include certain doctors' offices, hospitals, insurance companies, and others that electronically bill insurance companies. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

42 The data brokers share not only commercial sources but government and other publicly available sources as well.

Exhibit 2:

Data Sources

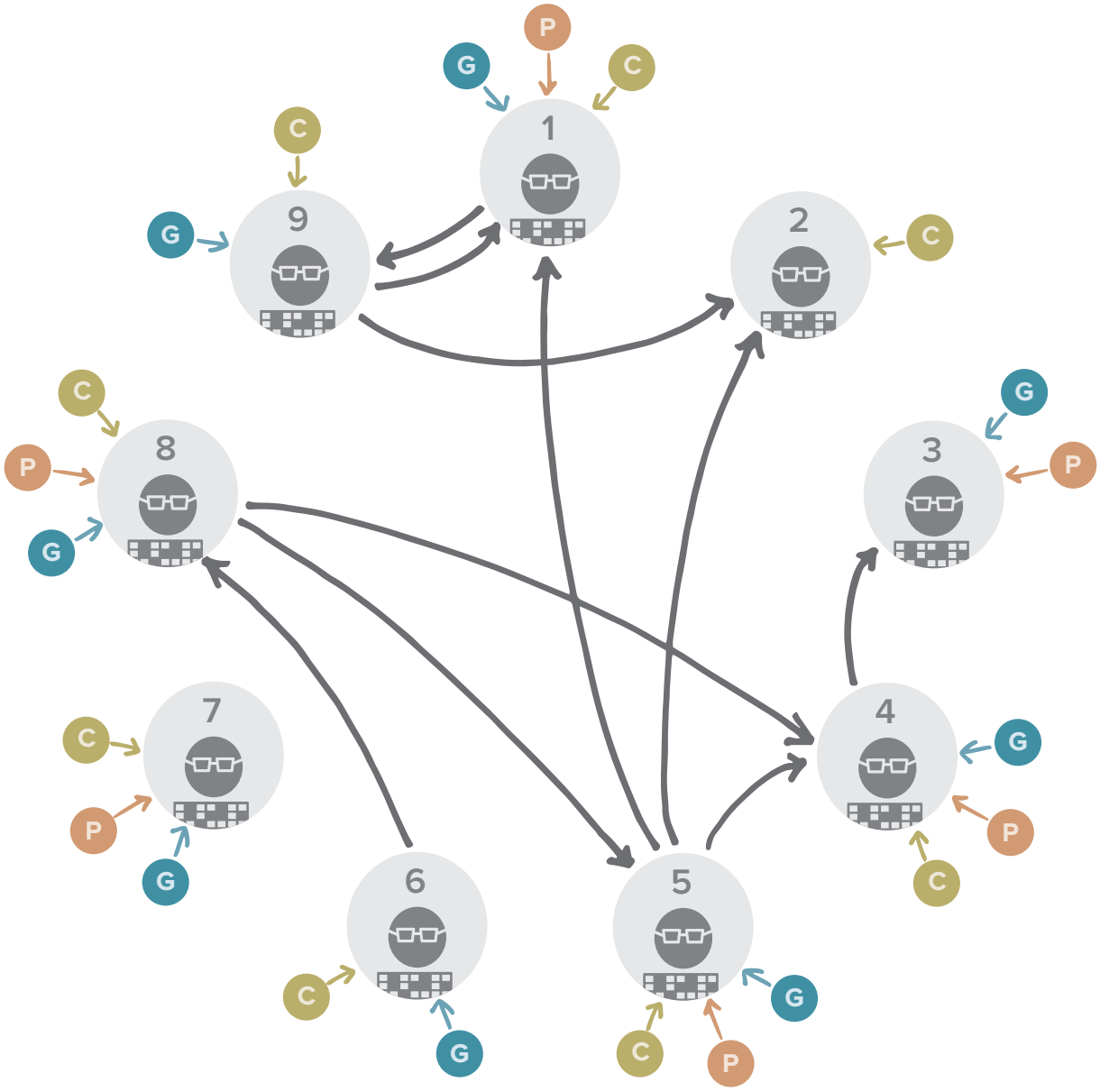
The nine data brokers the FTC studied collect information from many sources.*

data brokers in the study

government sources†

publicly available sources‡

commerical sources



* The Commission issued identical Orders to File Special Reports ("Orders") to nine data brokers under Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. § 46(b), to seek information about the data brokers' practices related to consumer data collection and use.

† Includes data brokers that sell information from government sources.

‡ Includes data brokers that sell information from publicly available sources.

B. Assessing Sources

While the data brokers in this study do not typically take steps to assess government and other publicly available sources, they may take some steps to assess their commercial sources in order to ensure that the sources provide accurate data. The majority of the data brokers in this study selects these sources based on their reputation in the industry. A few, however, affirmatively evaluate the legitimacy, stability, and quality of their sources before accepting data from them. This credentialing process may include reviewing the source's website, terms of use, data collection methods, privacy policy, privacy practices, and regulatory compliance. A few of the data brokers ask the source for its sources and then evaluate the original sources' websites, terms of use, privacy policies, and collection methods.

Several of the data brokers test the reliability of the information their sources provide up front. When they acquire a new data source, they put the new data in a holding area and test it to make sure it is internally consistent, corroborated by other sources, verifiable as legitimate, and that it encompasses a sufficiently large portion of the population.[43] Part of the testing process may include comparing the data against known truths (e.g., comparing the actual birthdate of the data broker's employee to the birthdate provided by the source). It may also include comparing the data to that obtained from other high-quality sources. Other data brokers assess the reliability of the data on an ongoing basis. They rely on automated systems that detect material deviations in their data and identify the sources that are causing such deviations. If there are discrepancies in the data obtained from two separate sources, some data brokers will use the data from the source they trust the most.

C. Contracts with Sources

The data brokers often enter into a variety of written contracts with their data sources. The data brokers may acquire *ownership* of the data under a data supply contract, *use* of the data for a defined time period under a data licensing agreement, or the *right to resell* the source's product using the data broker's brand under a data reseller agreement. These contracts generally include a description of the data provided to the data broker, the method for transferring the data, the frequency of updates, and any restrictions on using the data.

The contracts between the data brokers and their data sources include a range of provisions. Most of the data brokers insert provisions in these contracts stating that the data source warrants that it legally obtained the information. Only two of the data brokers insert contractual provisions requiring the data source to warrant that either it or its sources provided consumers with notice that their information would be shared with third parties and an opportunity to opt out of that sharing. At least one of these two data brokers appears to review the original source's website, terms of use, and privacy policy to determine whether

43 For example, before acquiring data on "Soccer Moms," the data broker will want to verify that this source has data on 10,000 "Soccer Moms," rather than just 100 "Soccer Moms."

the source provided consumers such notice and opt out opportunity. These contractual provisions do not contain requirements about the prominence of the notice or opt out, which the source may include in a privacy policy. Finally, the data brokers' contracts with their sources generally do not address the accuracy of information provided beyond noting that the sources will make best efforts to ensure accuracy.

The contracts also often contain use restrictions on data brokers. For example, certain federal or state laws or agencies require a written agreement affirming that the data broker will only use the data for a specified purpose. Sources may also prohibit data brokers from reusing or reselling the data without permission; decoding or reverse engineering the data; illegally or illicitly using the data; and using the data in violation of the FCRA,[44] Gramm-Leach-Bliley Act ("GLBA"),[45] HIPAA,[46] or Children's Online Privacy Protection Act ("COPPA").[47]

D. Collection Methods

The data brokers in this study collect information from sources in numerous ways. First, some data brokers collect publicly available web-based data through web crawlers, which are programs that capture content across the Internet and transmit it back to the data broker's servers.[48] The data brokers use software to determine which websites to crawl, how often, and what data points to collect from each website. Second, some data brokers buy or acquire printed information, such as telephone directories or local government records, and either scan these documents into an electronic format or have data entry professionals manually create an electronic record. Third, some data brokers arrange for batch processing of information. For example, some data brokers acquire data from their sources through a daily feed. Finally, the data brokers may arrange for their sources to make available to them an Application Programming Interface ("API") through which to process the data.

Whatever the method, it appears that the data brokers often collect more information than they use. Several of the data brokers reported that they cannot obtain a subset of data elements they request. For example, some sources sell the data brokers a multitude of data elements as part of a fixed data set even if the data broker does not need all of these elements. The data brokers may try to use the additional data elements in some other way, such as for matching or authentication purposes or to create models to predict consumer behavior. Or they may not use the data at all.

44 15 U.S.C. §§ 1681–1681v.

45 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.).

46 Health Insurance Portability and Accountability Act, 110 Stat. 1936.

47 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012).

48 As noted in supra note 40, some websites restrict or prohibit web crawlers from collecting data from their sites.

E. Data Updates

The data brokers' sources generally dictate the frequency of update schedules. Sources may update data either in real time, daily, weekly, monthly, quarterly, biannually, annually, or, in some limited instances, never. Data that is available through crawling or an API is typically updated more frequently than data acquired through, for example, batch processing or other non-automated collection methods.

Even if a source updates its data on a frequent basis, the data broker may not update its databases to reflect this new information immediately. There is typically a delay between when the data broker receives updated information from a source and when the data broker's system reflects this updated information.[49] Such a delay may occur because it is more cost effective for the data broker to update its databases at scheduled intervals rather than as each new data set is received. Or a delay may occur because the data broker is testing the data for accuracy. For example, when a source updates its data, the data broker may compare the source's newest file with its previous files for deviations that could affect accuracy. If the data broker obtains a substantially smaller file from a source that had previously provided a larger file, the data broker may discover that the source failed to provide information for all consumers with last names beginning with "A." When the data broker discovers such an omission, it may contact the source and ask for a new updated file.[50]

49 One data broker reports that it is upgrading its technology so that its system will update in real time.

50 Some of the data brokers report that they perform similar reviews of their own data to ensure that their databases reflect the most accurate data. For example, after updating its database to reflect an update from a source, a data broker might discover that its database is substantially smaller than the previous version of the database. In comparing the files, the data broker might discover that it failed to upload information about consumers residing in California.

III. DEVELOPMENT OF PRODUCTS

A. Creation of Data Elements and Segments

In developing their products, the data brokers use not only the raw data that they obtain from their sources, such as a person's name, address, home ownership status, age, income range, or ethnicity ("actual data elements"), but they also derive additional data ("derived data elements"). For example, a data broker might infer that an individual with a boating license has an interest in boating, that a consumer has a technology interest based on the purchase of a *Wired* magazine subscription, that a consumer has an interest in shoes because she visited Zappos.com, or that a consumer who has bought two Ford cars has loyalty to that brand.

The data brokers in this study sell both the actual and derived data elements to their clients. For example, elements they sell about Jane Doe may include her name, her age (36), her marital status (married), her interests (children and recreational sports), and her residence (123 Main Street). They may also use the actual and derived data elements to put consumers in categories ("data segments").

The data brokers create segments by:

- **Combining data elements to create a list of consumers who have similar characteristics.** Soccer Moms, for example, might include all women between the ages of 21 and 45, with children, who have purchased sporting goods within the last two years; or
- **Developing complex models to predict behaviors.** The data brokers can identify a group of consumers that has already bought the products in which the data broker wants to predict an interest, analyze the characteristics the consumers share, and use the shared characteristic data to create a predictive model to apply to other consumers. For example, a data broker can:
  - Analyze the characteristics of a subset of consumers that purchased camping gear in the last year, identify consumers in its database that share these characteristics, and create a segment called "Consumers Interested in Buying Camping Gear;"
  - Identify a group of consumers that sought chargebacks on their credit cards in the last year, analyze the characteristics those consumers share, and use the characteristic data to predict "Consumers that are Likely to Seek a Chargeback;" or
  - Analyze data on consumers in this manner to predict which consumers are likely to use brand name medicine, order prescriptions by mail, research medications online, or respond to pharmaceutical advertisements.

Some segments primarily focus on minority communities[51] with lower incomes, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latino and African-American consumers with low incomes.[52] Other segments highlight older consumers with lower incomes. For example, "Rural Everlasting" includes single men and women over the age of 66 with "low educational attainment and low net worths," and "Thrifty Elders" includes singles in their late 60s and early 70s in "one of the lowest income clusters." Yet other segments focus purely on consumers' financial status, such as "Underbanked Indicator," "Credit Worthiness," "Invitation to Apply Offers – Bankcard Utilization Rate," "Invitation to Apply Score," "Consumer Prominence Indicator," "Pennywise Mortgagees," and "Number of Orders – Low Scale Catalogs." Finally, other segments showcase a consumer's interests, such as "Truckin' & Stylin'" and "Health & Wellness Interest."[53] While some of these segments seem innocuous, others rely on characteristics, such as ethnicity, income level, and education level, which seem more sensitive and may be disconcerting.

51 Some of the data brokers offer an "Assimilation Code," which indicates a consumer's degree of assimilation to the English language.

52 Other segments focusing on a combination of ethnicity and/or income levels include: (1) "Work & Causes," which includes consumers "with lower-incomes, in their late 40s, early 50s," "living in multi-unit dwellings;" (2) "Resolute Renters," which includes consumers in their 30s and 40s, single with no children, that are "relatively mobile renters and on the lower rungs of income and net worth;" (3) "Metro Parents," which includes consumers, "primarily in high school or vocationally educated," "handling single parenthood and the stresses of urban life on a small budget;" (4) "Modest Wages," which includes "low-income singles living without children in a mix of smaller, industrial cities" with low "educational attainment;" (5) "Kids and Rent," which includes "lower income households" with children that are "mostly renters, living in both single-family and multiple-family apartment buildings;" (6) "Downtown Dwellers," which includes "lower-income, single, downtown-metro dwellers," that are "upper-middle-aged" and with a "high-school" or "vocational/technical" degree working to "make[ ] ends meet with low-wage clerical or service jobs;" (7) "Financially Challenged," which includes consumers "[i]n the prime working years of their lives, . . . including many single parents, struggl[ing] with some of the lowest incomes and little accumulation of wealth." These consumers are "[n]ot particularly loyal to any one financial institution, [and] they feel uncomfortable borrowing money and believe they are better off having what they want today as they never know what tomorrow will bring;" (8) "Timeless Traditions," which includes "immigrants, many of retirement age, . . . who have been in the country for 10 or more years," that "speak[ ] some English, but generally prefer[ ] Spanish," and that have "lower than average" incomes; (9) "Traditions & Timecards," which includes consumers with "an average age of 53" that "are still working" and that are the "least acculturated Hispanics, residing in more metro areas;" and (10) "Latchkey Leasers," which includes consumers with "an average age of 52" that are "predominately single renters living in multiple unit dwellings." This group tends "to be bicultural and bilingual," and "they earn some of the lower incomes and have relatively little net worth accrued at this point in their lives."

53 The data brokers offer a variety of segments, including at the individual, household, and zip code levels.

Segment Examples

- Financial Newsletter Subscriber
- African-American Professional
- Affluent Baby Boomer
- Spanish Speaker
- Outdoor/Hunting & Shooting
- Allergy Sufferer
- Santa Fe/Native American Lifestyle
- Senior Products Buyer
- Twitter User with 250+ Friends
- Media Channel Usage - Daytime TV
- Bible Lifestyle
- New Age/Organic Lifestyle
- Plus-size Apparel
- Biker/Hell's Angels
- Leans Left
- Exercise - Sporty Living
- Working-class Mom
- Upscale Retail Card Holder
- Modest Wages
- Financially Challenged

B. Data Suppression

Most of the data brokers exclude or suppress certain data from their products in several ways.[54] For example, they obtain suppression lists, such as the Commission's Do Not Call registry, to determine which data elements to mark as suppressed when processing the data that they acquire. Some of the data brokers reported that they have a policy against collecting or using information about children or teens.[55] Some of these data brokers rely on their sources to suppress the information, but do not take any additional steps. Others take additional steps to double check that the source has properly suppressed the information; they search the age, age range, or date of birth information to identify records of children or teens, filter out those records, and suppress any other records they associate with that same child or teen in the products they provide to their clients.

54 The data brokers use the term "suppress" to indicate that, although certain data may appear in their databases, they prevent the data from being included in their products. This section does not address consumer opt-out requests which, as discussed in Section VII.A., *infra*, also result in the data brokers suppressing data from their products.

55 Some of the data brokers intentionally include or factor in children's and teens' information in certain products. The data brokers that provide risk mitigation products used to detect fraudulent activity in commercial transactions, for example, may flag for a mobile telephone provider that an applicant's personal information belongs to an individual under the age of 18 and that the transaction may be fraudulent.

C. Data Storage

Three of the data brokers reported that they store data in the form of individual consumer profiles. For these data brokers, Jane Doe's file may contain her contact and demographic information, interests, and purchasing habits.[56]

Two of the data brokers store data by listing "events" in a database. For example, rather than having a profile of Jane Doe, they may have a long list of events such as:

- Jane Doe opened an account with ABC Bank on August 2 and listed her address as 123 Main Street;
- 123 Main Street was associated with a fraudulent transaction on September 23;
- John Smith moved to 123 Main Street on July 3;
- Mark Nobody was reported as deceased on December 21; and
- Mark Nobody opened a new mobile telephone account on December 31 and listed his address as 123 Main Street.

When these data brokers run a query on "Jane Doe," they can create a profile on her. For example, these brokers can determine not only that Jane Doe lives on 123 Main Street and that she has an ABC Bank account, but also that her address has been associated with multiple, potentially fraudulent transactions.

Two of the data brokers maintain databases that correspond to the sources of the data. For example, a data broker may have one database containing "court records" and another containing "real estate transactions." Some of the data brokers maintain databases that correspond to a product line; for example, a data broker may have a database for all of the data that is used in its risk mitigation products and another database for the data used in its marketing products, even if the data is duplicative. (These types of products are described in Section IV., *infra*.)

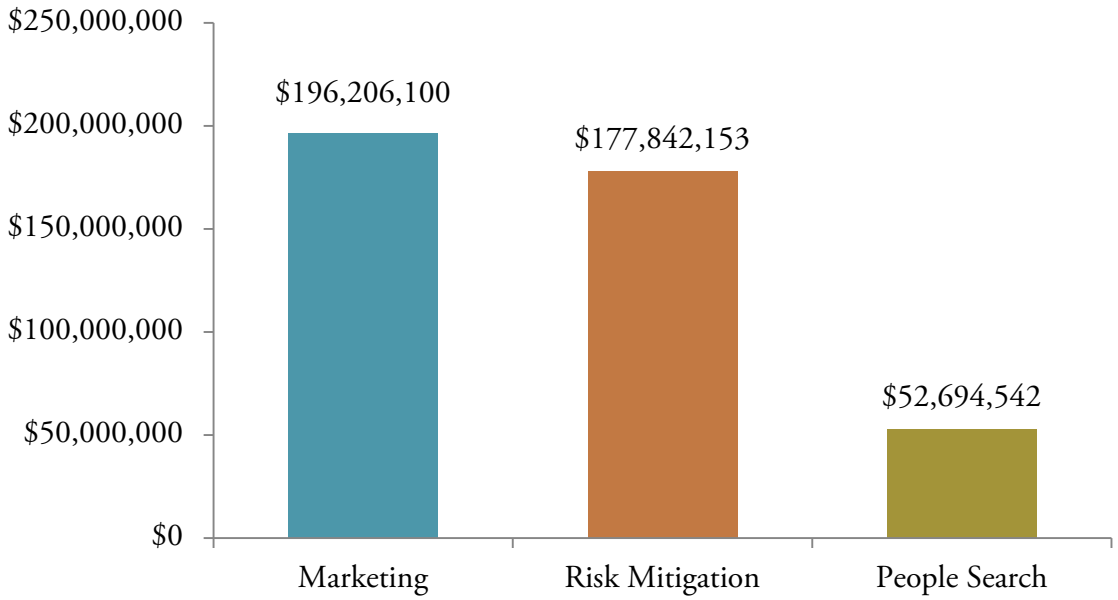
As to the length of retention of data, some of the data brokers store all data indefinitely, even if it is later amended, unless otherwise prohibited by contract. For some products, these data brokers report that they need to keep older data. For example, they explain that even if a consumer's address is outdated, it is important to keep the consumer's address history in order to verify his or her identity. For other products, however, retention of older data may not be necessary. An older address, for instance, is less relevant to deliver marketing to a consumer.

56 Rather than using names, some of these data brokers store individual consumer profile information using unique identification numbers.

IV. TYPES OF PRODUCTS

The data brokers offer products in three broad categories: (a) marketing; (b) risk mitigation; and (c) people search. These products generated a combined total of approximately $426 million in annual revenue in 2012 for the nine data brokers. The following graph depicts the proportion of revenue contributed by each type of product category.

Exhibit 3: Revenue of Nine Data Brokers by Product Category



A. Marketing

Five of the data brokers sell marketing products that collectively generated over $196 million in annual revenue in 2012. The Commission has grouped these marketing products into (1) direct marketing, which encompasses postal mail, telemarketing, and email marketing; (2) online marketing, which includes marketing to consumers on the Internet, on mobile devices, and through cable and satellite television; and (3) marketing analytics. All of these products enable the data brokers' clients to create tailored marketing messages to consumers.

1. Direct Marketing

Based on the information received, the Commission has identified two categories of direct marketing products: (a) data append; and (b) marketing lists.

a. Data Append

"Data append" products help companies learn more about their customers. They require the data broker's client to provide some customer information, such as name and address; the client can then select additional information—such as the customers' telephone number and purchasing habits—that the data broker appends to the client's data set for the client's use in direct mail, telemarketing, and email marketing campaigns.

Some products help clients fill in gaps that may exist in customer contact information. For example, the client may provide a customer's name and address, and the data broker could provide the customer's landline telephone number or email address. Alternatively, the client may provide the customer's landline telephone number, mobile telephone number, or email address, and the data broker could provide the customer's name and address. In some data append products, the client provides a customer's name and a store's zip code, and the data broker provides the customer's address.

Other products help clients better understand their customers. Clients may provide their customers' identifying information. The data broker can then append data to the clients' data sets. The data brokers in this study offer a large array of actual and derived data elements, including:

- Age
- Religious Affiliation
- Technology Interest
- Expectant or New Parent
- Gender
- Political Affiliation
- Social Media Usage
- Real Property Attributes
- Height
- Household Income
- Vehicle Ownership
- New Mover/Renter/Owner
- Weight
- Net Worth
- Credit Card Usage
- Discount Shopper
- Race
- Marital Status
- Vacation Habits
- High-End Shopper
- Ethnicity
- Biker
- Cholesterol Focus
- Home Loan Type
- Occupation
- Presence of Children

- Diabetes Interest
- Investment Habits
- Soon-to-be High School Graduates
- School-aged Children
- Smoker in Household
- Gambling
- Guns and Ammunition Purchases
- Home Ownership Status
- Buy Disability Insurance
- Lenses or Contacts
- Brand Medication Conscious

This information may include actual data elements, derived data elements, and data segments, as described in Section III.A. of this report. *Appendix B* provides an illustrative list of data elements and segments to demonstrate further the breadth of information available to clients.

b. Marketing Lists

Marketing lists identify consumers who share particular characteristics (e.g., all persons living with at least two children, all persons who are both women and own a specific car brand, people interested in diabetes, and households with smokers in them). The client identifies the attributes that it would like to find in a consumer audience, and the data broker provides a list of consumers with those attributes.[57] A client, for example, can request a list of consumers who are "Underbanked" or "Financially Challenged" in order to send them an advertisement for a subprime loan or other services.[58] Marketing lists can be limited to consumer names and addresses for direct mail campaigns, consumer names and telephone numbers for telemarketing campaigns, or consumer email addresses for email marketing campaigns. For clients who want more robust data to better tailor their marketing campaigns, the data brokers can include in the marketing lists any of the other data elements or segments described under the data append products. For example, a client can request a list of consumers in a particular region with an interest in gourmet cooking for a direct mail campaign and, in addition to the consumer names and addresses, the data broker can include in the marketing list the age or age range and household income of the consumers.

57 It has been reported that other data brokers, not part of this study, sell marketing lists identifying consumers who have addictions, AIDS and HIV, genetic diseases, or are police officers and troopers. *See, e.g.*, *Addictive Behaviors, Alcohol and Drugs Mailing List*, Exact Data, http://www.consumerbase.com/mailing-lists/addictive-behaviors-alcohol-and-drugs-mailing-list.html (last visited May 19, 2014); *Ailments Mailing Lists/Email Lists*, DMDatabases.com, http://dmdatabases.com/databases/consumer-mailing-lists/ailments-lists (last visited May 19, 2014); *Complete Medical's Ailments, Illnesses and Medical Conditions Mailing List*, Nextmark, http://lists.nextmark.com/market?page=order/online/datacard&id=221569 (last visited May 19, 2014); *Police Officers By District Mailing List*, Nextmark, http://lists.nextmark.com/market?page=order/online/datacard&id=330218&trk=y&aId=1381 (last visited May 19, 2014). *See also What Information Do Data Brokers Have on Consumers, and How Do They Use It? Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. (2013) (statement of Pam Dixon, Executive Director, World Privacy Forum), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=e290bd4e-66e4-42ad-94c5-fcd4f9987781.

58 Even though these categories may implicate creditworthiness, the use of data about a consumer's financial status in order to send the consumer targeted advertisements is generally not covered by the FCRA, unless the advertisements are for certain pre-approved offers of credit.

2. Online Marketing

Three of the data brokers facilitate the online marketing of products to consumers through the Internet, mobile devices, and cable and satellite television. The Commission has grouped the online marketing products into the following categories: (a) registration targeting; (b) collaborative targeting; and (c) onboarding. As discussed below, these practices permit companies to provide more targeted and potentially relevant advertising to consumers.

a. Registration Targeting

The data brokers can help registration websites[59] promote products to consumers more effectively through a more customized user experience. For example, if a travel website, XYZ Travel, wants to promote particular products to its users on its website, it can send the data broker a list of its registered users, and the data broker can provide XYZ Travel with the vacation interests of those specific users. With this information, XYZ Travel can highlight for Jane Doe a particular vacation package to Hawaii based on Jane Doe's interest in tropical islands when she logs on to XYZ Travel's website.

If XYZ Travel does not want to customize its site to individual registered users but instead wants to sell third-party advertising space on its site, it can send the data broker a list of its registered users. The data broker can then inform XYZ Travel that the majority of its registered users are interested in motorcycles and household cleaning products. With this information, XYZ Travel can offer to sell advertising space on its website to motorcycle vendors and cleaning product manufacturers.

The process works similarly for advertising on mobile devices and cable and satellite television. For example, Cable Company CBA can provide a data broker with a list of its registered customers, and the data broker can append that list with additional information about those customers. Cable Company CBA can use that information not only to market its own products—for example, to decide to which customers it should broadcast a promotional advertisement about its new Spanish-channels package—but also to offer third parties the ability to target advertising via these new Spanish channels. Specifically, Cable Company CBA may learn that a large subset of its Spanish-channels package subscribers enjoys international travel. Thereafter, Cable Company CBA can approach local travel agencies to purchase broadcast advertisements for those particular viewers.

b. Collaborative Targeting

Whereas in registration targeting, the data broker's client is the registration website, in "collaborative targeting," the data broker services two clients—the registration website and an advertiser looking to target advertisements on a registration website. The registration website gives the data broker a list of its users, and

59 "Registration websites," as discussed in Section II.A.3., *supra*, are websites that allow consumers to register or log in to obtain services, such as retail, news, and travel sites.

the advertiser gives the data broker its customer and prospect list. The data brokers report that neither party has access to personal information about consumers who are customers, potential customers, or registered users of the other. Only the data broker has access to both parties' information. The data broker can then analyze the data in order to enable the advertiser to decide whether to advertise on the registration website.

For example, Surfshop, a retailer of surfboards, wants to advertise a new surfboard and give its customers a discount through online advertisements. XYZ Travel offers Surfshop space on its website for a web banner, but Surfshop does not know whether its customers typically visit XYZ Travel. XYZ Travel and Surfshop do not want to share their customer lists with each other. XYZ Travel sends the data broker a list of its registered users, including names and email addresses. Surfshop sends the same data broker a list of its best customers, including names and postal addresses. The data broker appends email addresses to the Surfshop list and identifies 3000 Surfshop customers that are registered on XYZ Travel's website. Satisfied with these numbers, Surfshop sends the data broker the advertisement it wants to display on XYZ Travel's website, which in turn sends the advertisement to XYZ Travel. XYZ Travel displays Surfshop's advertisement to visitors of the site.

c. Onboarding: Combining Online and Offline Data

While collaborative targeting allows advertisers to determine which campaigns to run on particular registration websites, the practice of onboarding goes further. "Onboarding" refers to a process whereby a data broker adds offline data into a cookie (the process of onboarding offline data) to enable advertisers to target consumers virtually anywhere on the Internet. It allows advertisers to use consumers' offline activities to determine what advertisements to serve them on the Internet.[60]

Onboarding clients either (1) provide data about their customers to a data broker to facilitate the process of finding those consumers on the Internet to deliver targeted advertisements; or (2) use a data broker to identify an audience of consumers who are likely to share particular characteristics and find those consumers on the Internet to deliver advertisements. Three of the data brokers offer an onboarding product. Onboarding typically includes three steps: (i) segmentation; (ii) matching; and (iii) targeting.

i. Segmentation

The onboarding process starts when a client asks a data broker to find consumers with particular characteristics. Data brokers may have stock data segments that they have created based on anticipated client demand or they may create custom segments based on the client's request. For example, a data broker could help a clothing retailer advertise its new luxury fashion line to consumers online in several ways:

60 Some of the data brokers are also offering their onboarding services to clients so they can serve targeted advertisements on mobile devices.

- **To target the retailer's existing customers:** The retailer gives the data broker its customer list and the data broker compares its stock segments, such as "Persons Interested in High-End Clothing" or "Sophisticated Shoppers," to the retailer's existing list of customers to predict which of the retailer's customers will be interested in the new fashion line. If the data broker does not have a stock segment that fits the retailer's needs, the data broker can create custom segments based on the retailer's criteria. For example, the retailer might want to target its line to all of its existing customers who are "Women" living in the "Zip Code 12345." After creating the segment, the data broker would compare individuals in the customized segment to the retailer's customer list and identify those existing customers best suited for the retailer's advertising campaign.
- **To target new customers for the retailer:** The data broker may also offer the retailer access to the data broker's own list of segments to find new customers. The retailer would select one or more stock segments (e.g., "Sophisticated Shoppers" or "Persons Interested in High-End Clothing"), and the data broker would then identify consumers from its own databases that fit within these segments. If none of the data broker's stock segments fit the retailer's needs, the data broker can simply customize a segment (e.g., "Women" that are living within "Zip Code 12345") and apply that segment to the data broker's database of consumers.

ii. Matching

The next step in the onboarding process is "matching," where the data broker finds the consumers it identified through the segmentation process online. To find consumers online, the data broker enters into contracts with registration websites to buy lists of registered users. It then compares these registered users with the consumers identified through the segmentation process in order to find matches. When the data broker finds a match, it appends to that consumer any data elements or segments associated with the consumer.[61]

Thus, in the example of the clothing retailer looking to advertise its new luxury clothing line, suppose the data broker comes up with 100,000 consumers meeting the criteria of the clothing retailer, including Jane Doe. Suppose further that the data broker has bought Social Media X's registered users list. If the data broker finds that Jane Doe is a registered user of Social Media X, it has found a match. The data broker thereafter can associate Jane Doe with the data elements and segments requested by the client (e.g., "Woman," "Zip Code 12345," and "Sophisticated Shopper").

61 The data brokers represent that they typically do not store the consumer's name, but maintain a unique identifier for each consumer. The entire matching process is conducted using unique identifiers, rather than consumer names.

iii. Targeting Consumers Online

The last step in the onboarding process is to target the matched consumers online. To do so, the data broker must first place a cookie on the browsers of the consumers it has identified through the above process. It does so when the registration website notifies the data broker that such a consumer has logged on to the registration website. The cookie includes the information that the data broker has appended to the consumer's profile, but the data brokers reported that it does not include other more traditional forms of identifying information, such as name, email address, or postal address.

Once the data broker has placed a cookie on the consumer's browser, the data broker can advertise to the consumer across the Internet for as long as the cookie stays on the consumer's browser. The data broker either acts as an advertising network itself by buying advertising space on various websites or contracts with advertising networks that have secured advertising space on these websites. In this way, the data broker can place a cookie on Jane Doe's browser, add to the cookie that she is a "Woman," living in "Zip Code 12345," and a "Sophisticated Shopper," and serve her an advertisement within the data broker's partner network, either on behalf of the fashion retailer or any other one of its online or offline clients.

In addition to the example described above, data broker clients can use onboarding products in several additional ways:

- **Retargeting.** A retailer may want to use its existing customer and prospect lists to present those consumers with specific offers across the Internet. For example, a lender may want to target its financially distressed customers for a new subprime credit card, or a hotel might want to target its high-value rewards members to advertise a vacation getaway.
- **Cross-Channel Campaigns.** A retailer may want to target an identical audience through multiple channels. For example, a pet store may want to run a campaign to sell a new dog shampoo to dog owners simultaneously via direct mail, email, and Internet advertisements. Through onboarding, the pet store can find on the Internet the customers to whom it sent its direct mail and email brochures and target them with Internet advertisements as well.

Finally, although some of the studied data brokers are onboarding consumers' *offline* activities to advertise to them *online*, they do not appear to be using consumers' online web browsing activities to target them offline. However, one of the data brokers stated that its customers have asked for this functionality and that it plans to offer it in the future. A review of the privacy policies of other data brokers that were not part of this study demonstrates that some data brokers may be already using consumers' web browsing activities in offline direct marketing products.[62]

62 *See, e.g.*, *Privacy Policy*, FiveData, http://fivedata.com/privacy.html (last visited May 19, 2014); *Privacy Policy*, eTargetMedia, http://www.etargetmedia.com/privacy.html (last visited May 19, 2014).

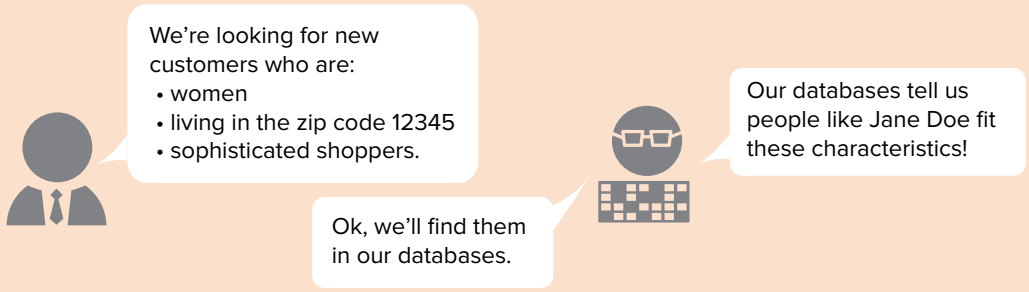
Exhibit 4:

Onboarding

When data brokers help businesses find consumer targets for online advertising.

1 Segmenting

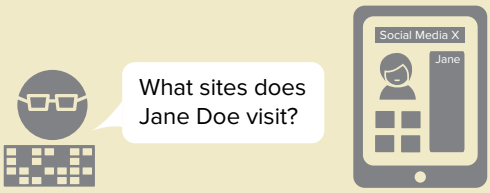
A business asks a data broker to find consumers with particular characteristics.



2 Matching

The data broker finds the targeted consumers online,

assigns Jane Doe to the targeted segment,



and finds Jane Doe is registered on Social Media X.

3 Targeting

The data broker uses cookies to display the business's ads on sites the targeted consumers visit.

Next time Jane Doe logs on to Social Media X, the data broker places a cookie on her browser.

When Jane Doe visits certain websites, the business's ads may be displayed.

3. Marketing Analytics

Five of the data brokers in this study provide analytics for marketing purposes, as a way to predict consumers' likely behavior. Among other things, the analytics products offered by some of the data brokers enable a client to more accurately target consumers for an advertising campaign, refine product and campaign messages, and gain insights and information about consumer attitudes and preferences. For example, some data brokers will analyze their client's customer data and advise a client regarding the type of media channel to use to advertise a particular product or brand (e.g., online, newspapers, television) and where the advertisements should be shown (e.g., Florida or California). As part of this analysis, the data brokers can also help their clients model the expected outcomes of various marketing tactics, thus allowing the clients to better advertise their products to consumers. For example, a data broker might be able to predict whether advertising a new product exclusively through Twitter will yield the desired outcome.

Some of the data brokers offer their clients the ability to evaluate the impact of an advertising campaign after it has run. These analytic products are generally based on algorithms that consider hundreds or thousands of data elements, including historical data provided by the client and data that the broker gathers from the government, other publicly available sources, and commercial sources described above. For example, after a telecommunications company runs an online advertising campaign for its newest mobile device, that company might want to know how many of its customers saw those advertisements, went into a physical store, and purchased that device.

Some of the data brokers convert their analyses into a variety of different marketing scores for consumers. Some scores rank clients' customers on the basis of how likely they are to respond to particular marketing efforts. For example, clients may rely on marketing scores to identify consumers or addresses on direct mail lists with a low response rate. Clients may also rely on marketing scores to identify addresses that have a high undeliverable mail rate or consumers with a low purchase rate. These types of scores could be used to determine the types of offers consumers may receive, the number of offers, or even the level of customer service provided to specific individuals. Other scoring products measure a consumer's presence on the Internet or a consumer's influence over others. These scores are based on, for example, the consumer's blogging practices, participation in social media sites such as Facebook and Twitter, the number of friends, followers, or readers the consumer has, the amount of content the consumer creates on the Internet, or the consumer's prominence in the news. Clients may use these social influence scores to ensure that they advertise their products to these particular consumers, with the expectation that these consumers will, in turn, tout these products to their friends and followers.[63]

63 On March 19, 2014, the FTC hosted a seminar on alternative scoring products, as part of a series of seminars to examine the privacy implications of new areas of technology. *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. The seminar included discussions about the scores discussed in this report. *Id.* (transcript available at www.ftc.gov/system/files/documents/public_events/182261/alternative-scoring-products_final-transcript.pdf).

B. Risk Mitigation

Four of the data brokers sell risk mitigation products that generated approximately $177 million in annual revenue in 2012. The Commission has grouped these products into two categories: (1) identity verification and (2) fraud detection.[64]

1. Identity Verification

In general, identity verification products assist clients in confirming the identity of an individual. The data broker clients use identity verification products for diverse reasons. For example, banks use such products to comply with "know your customer" identity verification requirements under the USA PATRIOT Act[65] or to otherwise help deter fraud at the time a consumer commences a transaction.

Some of the data brokers offer identity verification products in several formats. First, the data brokers offer a scoring format, in which the client receives a numerical score indicating the level of risk associated with the transaction, along with explanatory codes that relate to the calculation of the score. For a consumer with a high risk score, the explanatory codes could state that the SSN provided by the consumer is associated with a deceased individual, the address used by the consumer has been associated with fraud or is a prison address, the SSN has been used very frequently in a short period of time, or the SSN has been attributed to an address other than the one submitted by the consumer.[66]

Second, as a standalone product or to provide an additional layer of authentication, the data brokers offer their clients a quiz product, which typically includes questions to which the answers should be easily known to the consumer, but would not likely appear in information stolen by an identity thief, such as information that can be found in the consumer's wallet. Questions might include: "Which of these is an email address you have used?" or "What is your mother's birthday?" When used in conjunction with a scoring product, if a consumer scores high on risk, the data broker's client may require the consumer to answer five out of the six questions correctly; however, if the consumer's risk score is low, the data broker's client may only require that the consumer answer three of the six questions correctly.

64 As noted earlier, the Commission's Orders to the nine data brokers did not seek information about data broker activities that fall within the scope of the FCRA. However, some risk mitigation products could be covered by the FCRA, depending upon the information collected and its use. The Commission has previously sent warning letters to data brokers that appeared willing to sell data for FCRA purposes but did not consider themselves to be subject to the FCRA. *See* Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations. The Commission will continue to focus on this issue.

65 Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 31 C.F.R. § 1020.220 (implementing Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001)).

66 The data brokers use the SSN to create these types of products, but do not share the SSN with their clients.

Third, the data brokers offer the "match/no match" format, which provides confirmation that information provided by the consumer matches the information in the data broker's files. In some cases, the data broker may provide a "close match" option, where, for instance, two digits in the telephone number look like they may have been transposed.

Some of the data brokers provide a category of identity verification products called a status verification product, which serves to both identify an individual and indicate a status of that individual. Status verification products can ascertain whether a person is active duty military personnel and thereby entitled to certain foreclosure protections[67] or whether an individual is listed as an excluded party for purposes of government contracting or procurement.[68] They also include products that provide verification of employment (e.g., that *X* consumer works for *Y* employer).

2. Fraud Detection

Some of the data brokers also sell products to help their clients identify or reduce fraud. For example, one data broker offers a product that indicates whether an email address has existed for a period of time or has a history of transactions related to it. Another data broker tracks address information to assist companies in detecting patterns associated with attempted fraud (e.g., the delivery address is not associated with the listed consumer).

Fraud detection products also can assist entities in verifying the reliability or truthfulness of information a consumer submits to them. For example, if a public benefit is contingent on a consumer's level of income, a consumer may fill out a form declaring his or her income. The data brokers can provide a general confirmation of such income (inferred from broad demographic data) or, with the consumer's consent, can verify the individual's income based on his or her Internal Revenue Service tax return.

Data broker products also can assist companies that have had a data breach by analyzing patterns to determine whether there appears to be misuse of the personal information breached. For example, if the breach included employees' SSNs, the company can provide the data broker with a list of those SSNs

67 *See* Servicemembers Civil Relief Act, Pub. L. No. 108-109, 117 Stat. 2835 (2003) (codified at 50 U.S.C. app §§ 501–596). The protections of this statute apply to active duty military personnel who had a mortgage obligation prior to enlistment or prior to being ordered to active duty.

68 As a means of protecting public funds from fraud and abuse, governmental entities and certain others publish lists of individuals and entities that are excluded or barred from receiving government benefits, contracts, financial assistance, or funds. Such exclusionary lists have been maintained by General Services Administration. *See* System for Award Mgmt., https://www.sam.gov/portal/public/SAM/##11 (last visited Mar. 26, 2014) (The General Services Administration discontinued the Excluded Parties List System on November 21, 2012. Exclusions are now maintained by the System for Award Management); U.S. Department of Health & Human Services, *see Exclusions Program*, Office of Inspector General: U.S. Dep't of Health & Human Servs., https://oig.hhs.gov/exclusions/index.asp (last visited Mar. 26, 2014) (setting forth a list of individuals and entities excluded from participating in Medicare, Medicaid, and any other federal health care program); Freddie Mac, *see How to Access Freddie Mac's Exclusionary List in Loan Prospector*, Freddie Mac (Sept. 2008), http://www.freddiemac.com/learn/pdfs/uw/ex_lst_lp.pdf (setting forth list of individuals and entities excluded from participating in transactions involving Freddie Mac loans); and others.

and ask the data broker to monitor whether a particular SSN on the list is suddenly associated with many different addresses, thereby suggesting fraud.

C. People Search

Three of the data brokers provide people search products, which generated over $52 million in combined annual revenue in 2012. "People search" products offer information about consumers obtained from government and other publicly available sources, such as social media sites, as described above. These products are unique in that they are often intended for use by individuals, although they can be used by organizations as well. Users utilize people search products for such purposes as tracking the activities of executives and competitors, finding old friends, researching a potential love interest or neighbor, networking, or locating court records. People search products provide personal information about consumers. These products may allow a user to conduct a search with as little as one data element, such as name, address, city/state, telephone number (including mobile telephone number), email address, username, or SSN. The products provide a variety of information including:

- Aliases
- Age and date of birth
- News stories
- Telephone number
- Gender
- Interests/affiliations
- Address history
- Education information
- Death records
- Relatives
- Employment history
- Marriage records
- Email address
- Criminal records
- Divorce records
- Civil records (including bankruptcies, liens, judgments)
- Property ownership and sales history (including loan activity)
- Social media information (including usernames, profile URL, friend connections)
- Neighbors (including sex offenders)

Some of the data brokers provide free search products, and other data brokers provide fee-based products. In general, the data brokers instruct users that they cannot use these products for purposes

governed by the FCRA, including eligibility for employment, credit, insurance, housing, or similar purposes.[69]

69 The Commission has stated that a disclaimer alone will not suffice to keep a product outside the confines of the FCRA. *See* Complaint at 3, Filiquarian Publ'g. LLC, No. C- 4401 (F.T.C. Apr. 30, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130501filquariancmpt.pdf; Complaint at 5, United States v. Spokeo, Inc., No. CV12-05001-MMM-SH (C.D. Cal. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeocmpt.pdf.

V. DATA QUALITY

The procedures that the data brokers use to assure the quality of the data they provide to clients depend on the type of product at issue and the data broker's business model.[70]

A. Marketing Products

For marketing products to be effective, the data brokers generally need to provide information to their clients so that the relevant marketing message (e.g., a golf-related advertisement) reaches the correct consumer (e.g., golfer Jane Doe at 123 Main Street). To this end, they implement several procedures.

First, as described in Section II.B. of this report, they take steps to ensure the accuracy of the data they receive from their sources, so that, for example, consumers whom the source identifies as being interested in hiking are, in fact, interested in hiking. These steps range from relying on the reputation of their sources to affirmatively evaluating some of the data provided.

Second, they take steps to ensure that they are matching the correct information with the correct consumer in their database. The data brokers' matching practices vary. Some, for example, require stringent matching of the name and address elements. For example, if a source says that Jane Doe at 123 Main Street is interested in golfing, the data broker will only assign the golfing interest to the Jane Doe in its database who lives at 123 Main Street. Others rely on fuzzy logic[71] matching rules. These data brokers may assign the golfing interest to Jane Dae, rather than Jane Doe, if their files show that Jane Dae lives at 123 Main Street.[72]

Third, they may take steps to ensure that the identifying information they have is accurate and up-to-date. Some of the data brokers will attempt to fill in missing information, such as a middle initial on a name or a street suffix (e.g., Avenue or Terrace). A few data brokers will check an address to make sure that a move record is not associated with the individual and keep the most recent address. Several of the data brokers will delete a record if it shows up on the Death Master File.

Fourth, the data brokers may reconcile conflicting information. One data broker relies on mathematical algorithms to reconcile conflicting data elements. For example, if two data sources list a consumer's age as 25, another as 26, and two others as 25–35, the data broker might assign the age as 25 to that consumer.

---

70 The phrase "data quality" has traditionally been referred to as "data accuracy." For the reasons described in Section V.B., for some fraud detection products, having some inaccurate data is important in order to detect anomalies and potential fraud. Thus, this section uses the term "data quality."

71 Fuzzy logic matching rules allow a computer to find matches even where the search terms are misspelled. For example, a search for "Barack Obama" under fuzzy logic matching rules might retrieve information about "Barak Obama" and other related terms.

72 A similar matching process takes place when data brokers in this category sell data append products, where they have to associate information with a particular customer, as requested by the client.

Finally, several of the data brokers report that they accept inquiries from clients about data quality and attempt to take appropriate remedial action. These data brokers reported that data quality matters to their clients, who may terminate a data broker who provides less useful or accurate data than another data broker providing the same product. For example, if a data broker receives numerous complaints from its clients about the accuracy of the data, and the data broker determines that the information comes from a particular source, the data broker may further evaluate that source before obtaining updates or additional data from it.

B. Risk Mitigation Products

Like the data brokers that offer marketing products, the data brokers that provide risk mitigation products take steps to assess whether their sources are providing reliable information. (*See* Section II.B., *supra*). Unlike the data brokers that provide marketing products, however, for the most part, the data brokers selling fraud detection products avoid altering the data they obtain[73] and tend to retain historical and anomalous data in order to spot potential trends associated with fraud. For example, while a data broker that sells a marketing product may delete a consumer record if that consumer appears on the Death Master File, a data broker providing a fraud detection product will keep the data in the consumer's record to flag when a person using the deceased consumer's data attempts to open an account. Similarly, if John Doe attempts to use his SSN to apply for a mobile telephone contract and a data broker's fraud detection product shows that the same SSN belongs to another individual, then the transaction may be flagged as potentially fraudulent.[74] Eliminating the entries related to other consumers' use of John Doe's SSN may undercut the ability to detect or prevent fraud. Thus, while some data used in fraud detection products may not be current or accurate, that data may nevertheless be relevant for purposes of detecting possible fraud.

In contrast, for identity verification products, associating correct identifying information (often an SSN) with a particular individual is critical. The data brokers selling identity verification products tend to require precise matching before linking a data element to an individual. While a data broker selling a marketing product may match information to a consumer using only name and address, identity verification products are more rigorous. They rely not only on names and addresses, but may also require that the driver's license and SSN match the information in their records to ensure that the information relates to the correct individual. In this way, the data broker can try to ensure that, for example, John Doe, Senior, will not be denied the ability to complete a transaction because he has been misidentified as John Doe, Junior, who lives in the same house.

73 They may use standardization information to make data more consistent with U.S. Postal Service standards (e.g., they may change "North 32nd Street" in one file to "32nd Street North").

74 *See* Section VIII.B.2., *infra*, for a discussion of the FCRA's application to these products.

C. People Search Products

Unlike the data brokers in the other two categories, the data brokers providing people search products, for the most part, do not assess their sources because they primarily use publicly available sources. One data broker reported, however, that it compares the information acquired from publicly available sources to information acquired from other data brokers in order to assess the accuracy of the information.

The data brokers providing people search products report that they take steps to match the data they receive to the appropriate individual. For example, if a data broker finds a newspaper article relating to John Doe, and there are two John Does in its system, the data broker may look at the newspaper article to see if it mentions John Doe's place of residence or his age. In doing so, the data broker might be able to determine that the newspaper article relates to the John Doe living in California, rather than the John Doe living in Florida. One of these data brokers has patented a matching logic system to facilitate better matches.

In many cases, a user's search through one of these people search products will generate a number of different results. For example, a search for "Mike Smith" might provide results for "Michael Smith," "Mike D. Smith," "Micheal Smith," and "Mike E. Smith." Typically, the data brokers in this category will leave it to users to determine which results, if any, match the person they are seeking.

VI. CLIENTS

A. Types of Clients

Each of the data brokers studied has numerous clients. The following chart provides a snapshot of the main categories of data broker clients.

Exhibit 5: Clients by Product Type and Industry Sector

	Direct Marketing	Online Marketing	Marketing Analytics	Identity Verification	Fraud Detection	People Search
Alternative Payment Providers[i]				X	X	
Attorneys & Investigators	X					
Automotive Industry	X	X	X			
Consumer Packaged Goods Manufacturers[ii]	X	X	X			
Data Brokers	X	X	X	X	X	
Educational Institutions	X			X	X	
Energy/Utilities	X					
Government Entities	X		X	X	X	X
Hospitality/Travel/ Entertainment	X	X	X			
Individual Consumers						X
Insurance Companies	X		X	X	X	
Lenders/ Financial Services Firms	X	X	X	X	X	X

	Direct Marketing	Online Marketing	Marketing Analytics	Identity Verification	Fraud Detection	People Search
Marketing/ Advertising Firms	X	X	X	X	X	X
Media	X		X			X
Non-profit Entities/ Political Campaigns	X	X		X	X	
Pharmaceutical Firms	X		X			X
Real Estate Services	X				X	X
Retail Companies	X	X	X	X	X	X
Technology Companies[iii]	X	X	X			X
Telecom Companies[iv]	X		X	X	X	

[i] Alternative Payment Providers include companies who provide consumers with alternative methods of payment rather than traditional methods such as checks or credit cards.

[ii] Consumer Packaged Goods Manufacturers include companies that manufacture items that consumers use and have to replace frequently, such as food and beverages, apparel, and household products.

[iii] Technology Companies include hardware companies, software companies, Internet companies, and other technology companies.

[iv] Telecom Companies include telephone, mobile, cable and satellite television providers, and other telecommunication companies.

In addition, some of the data brokers, on a limited basis, have also sold information to companies in the debt collection and debt buying industries to help those companies locate individuals and/or determine the likelihood that they will repay a debt.

B. Client Screening, Contracting, and Monitoring Practices

The data brokers' client screening, contracting, and monitoring practices vary, depending on the type of product (e.g., marketing or fraud detection), the type of data provided by the product (e.g., property information or lifestyle data), or the type of client (e.g., financial institution or retailer). For example, when compiling government and other publicly available information to provide people search products to the

general public, the data brokers tend to engage in minimal screening or monitoring of their clients. Clients, including individual consumers, access these products through the data brokers' websites and the data brokers do not determine the purpose for which the client will use the product. The data brokers state that they prohibit certain uses of data through their websites' Terms of Use, which often include prohibitions on using the products for unlawful purposes, for FCRA purposes, or both. Some of the data brokers only post their Terms of Use on their websites without requiring clients to affirmatively agree to the terms; others require clients to affirmatively agree to the Terms of Use when completing the transaction, although the terms may not be displayed during the transaction. The data brokers generally do not review, monitor, audit, or evaluate the use of their people search products after the client completes the transaction.

Apart from the people search category, several of the data brokers engage in some screening and monitoring of their clients.[75] The screening process may include meeting or speaking with potential clients, relying on the well-established reputation of the potential client, and performing some research on the legitimacy of the potential client's business, such as verifying the business address, performing Internet searches, and reviewing the potential client's website. In addition, one data broker reported that it does not sell its products to clients involved in certain industries, such as pornography, debt repair, credit counseling, private investigation, or the sale of illegal drug products or services or illegal weapons.

A few of the data brokers engage in more significant screening and monitoring. In addition to the screening process described above, the data brokers may include a credentialing questionnaire to determine if the client is a legitimate entity and has a lawful use for the product, site inspection, security review, website review, and reference checks. These data brokers also include auditing provisions in their client contracts, perform audits of their clients, and have terminated clients for contract violations.

Whether or not they screen or monitor their clients, the data brokers that offer risk mitigation and marketing products enter into written, signed contracts with their clients that describe the permitted and prohibited uses of the product. Prohibited uses may include reuse or resale of the data without permission; decoding or reverse engineering of the data; illegal or illicit uses; uses in violation of the FCRA, GLBA, HIPAA, or COPPA; and uses in violation of industry self-regulatory guidelines.

The contracts between data brokers and their clients include few provisions regarding the accuracy of their products. Some of the data brokers represent to their clients that their information is only as accurate as their sources and accept no responsibility to validate the accuracy of their data. Other data brokers, rather than making representations regarding the accuracy of their data, focus on the utility and predictive quality of their products.

75 Notably, the IRSG principles discussed in the Introduction were designed to screen clients, in part to avoid misuse of data that IRSG member companies provided to their clients. However, the industry ultimately terminated the IRSG. *See* IRSG, *supra* note 5.

VII. CONSUMER CONTROLS OVER DATA BROKER INFORMATION

In the following sections, the Commission describes some of the salient features of the data brokers' access, correction, opt-out, and deletion policies by product type.

A. Marketing Products

Of the five data brokers that sell marketing products, four provide consumers with access to certain limited information.[76] These data brokers provide notice on their website, typically within a lengthy privacy policy, and an explanation of how to access the information; however, these notices may be hard to understand. In response to a consumer request, some of these data brokers will provide the consumer's name accompanied by a few general interest categories the data broker has associated with that consumer, such as "Travel Enthusiast" or "Green Consumer." Consumers are not provided access to all of the data that the data broker has associated with them and/or all of the inferences made from that data. The data brokers typically provide access to raw data and not to their proprietary information that they derive through algorithms. As a result, consumers may not know they have been categorized in a particular manner.

To the extent consumers can access information about themselves, they are required to submit personal information to verify their identity and sometimes additional documentation through postal or electronic mail, such as a physical or scanned copy of a government-issued photo identification card or passport, and, for one broker, possibly a copy of a recent credit, utility, or telephone bill.[77] The data brokers in this study report that they use this personal information only for authentication purposes and to process access requests.

Only two data brokers that sell marketing products allow consumers to correct their information. Of them, one data broker launched a new website in September 2013 that, among other things, lists some elements the data broker sells in its marketing products used for online advertising and enables consumers to correct some of these elements.

The four data brokers that sell marketing products and provide consumers with access also allow consumers to opt out of the use or sharing of their personal information for marketing purposes. Opting out means suppressing the consumer's personal information from display in the data broker's marketing

76 In September 2013, one data broker, Acxiom, publicly announced changes to its access policy after submitting its final responses to the Order. This data broker launched a new website to enable consumers to access and correct information about them, and to and opt out of having some information included in certain marketing products. *See* Press Release, Acxiom Corp., Acxiom Launches New Consumer Portal (Sept. 4, 2013), *available at* http://www.acxiom.com/acxiom-launches-new-consumer-portal/.

77 Despite recognizing that minors would not typically have such documentation, one data broker explained that it provides access only to consumers able to produce the documentation.

products. These data brokers generally do not delete the consumer's information from their systems. Instead, they maintain the information in order to be able to match records that they may receive in the future and identify which consumer records should be suppressed. Some data brokers also report that they might continue to use the suppressed information in products that display data in aggregated, anonymous form.

These four data brokers provide notice of their opt-out policy via their individual, company-specific websites, usually in the privacy policy. Consumers can submit opt-out requests through a web form that requires basic consumer contact information, such as name, mailing address, and possibly an email address. Some of the data brokers also accept opt-out requests by mail or fax. When compared with the data access requests, the data broker opt-out procedures appear to focus less on authentication of the individual and more on streamlining the process for both the data broker and the consumer. For example, opt-out requests generally do not require the submission of supporting documents. When consumers provide their personal information in order to opt out, the data brokers have indicated that they use the information only for the opt out.

The data brokers that provide consumers with the ability to opt out convey some limitations regarding opt outs to consumers, but do not convey others, which could confuse consumers. For example, among the three data brokers that sell risk mitigation and marketing products, one data broker's opt-out disclosures did not clearly convey that the opt out is limited to just the marketing products, which comprise a small percentage of the data broker's business.

Opting out typically does not take effect immediately. It often takes a data broker several weeks to suppress a consumer's personal information from its database. Furthermore, while a consumer may opt out, information about that consumer might still appear in another consumer's records, such as that of a spouse. In addition, if a consumer submits identifying information in an opt-out request that varies from the identifying information in the data broker's records, the opt out may not capture all of those records. For example, "Jonathan Doe" may not know to also submit for his shortened name, "Jon Doe." As a result, consumer opt-out requests may not be completely effective.

B. Risk Mitigation Products

Of the four data brokers that sell risk mitigation products, two provide consumers with some form of access to their information. In order to obtain their information, consumers are required to submit personal information to verify their identity, such as name, address, telephone number, email address, and possibly provide a photocopy or electronic scan of a government photo identification card and a copy of a recent credit card, utility, or telephone bill. As with data brokers selling marketing products, the data brokers providing risk mitigation products use this personal information only for authentication purposes and to process the access request. Depending on the data broker's procedures, consumers can submit access requests

by web form, mail, or email. One of the two data brokers charges a $5 processing fee for access. The two data brokers that provide consumers with access set forth a notice on their website, typically within their privacy policy, and provide an explanation of how to obtain the information. The two data brokers provide different levels of detail in their website notice. For example, one data broker describes a procedure to obtain the data used in its products generally, whereas the other data broker specifies a procedure for obtaining the data used in its risk mitigation products.[78]

Only one data broker allows consumers to correct their information. The others do not offer such an option, stating that it would undermine their efforts to detect fraud. None of the data brokers allows consumers to opt out of the use or sharing of their personal information in the data brokers' risk mitigation products.

C. People Search Products

The three data brokers that provide people search products provide access to consumers by allowing them to search for themselves by using the same free or fee-based products the data broker offers to its clients. One data broker that offers fee-based people search products provides consumers with free access to their own information, but consumers must verify their identity by responding to a number of knowledge-based authentication questions.

These data brokers also allow consumers to correct some information in varying degrees. One data broker allows consumers to correct their displayed email address, another data broker allows consumers to annotate their information by appending remarks to their profile, and the third data broker allows consumers to report facts as inaccurate, which prompts the data broker to check on the accuracy of its source and, if necessary, fix the inaccurate fact within twenty-four hours.

Two of the data brokers that provide people search products allow consumers to opt out of the disclosure of their information. One data broker requires that the consumer provide a copy of the consumer's driver's license—with the photo and license number crossed out—by mail or fax or uploaded through a web form, and the other data broker does not require any documentation. One of the data brokers indicated that it treats people search product-related complaints as opt-out requests even if the consumer does not specifically request to opt out. As with marketing products, opt outs for people search products may be incomplete. If a consumer submits identifying information in an opt-out request that varies from the identifying information in the data broker's records, the opt out may not capture all of those records. As a result, consumers may find themselves having to submit many opt-out requests to the same data broker.

78 One of the data brokers has been providing consumers access to the data used in its risk mitigation products for a number of years, while the other began in August 2012.

As to deletion, the three data brokers that provide people search products explained that they do not offer consumers the option to delete their information because such measures would be futile. They explained that, because they refresh their data via automated means such as web crawling, the same, similar, or seemingly related information about consumers that was deleted is otherwise publicly available and will reappear on the Internet and in their databases.

VIII. FINDINGS AND RECOMMENDATIONS

This report reflects the information provided in response to the Orders issued to nine data brokers, information gathered through follow-up communications and interviews, and information gathered through publicly available sources. Based primarily on these materials about a cross-section of data brokers, the Commission makes the following findings and recommendations:

A. Findings

1. Characteristics of the Industry

- **Data Brokers Collect Consumer Data from Numerous Sources, Largely Without Consumers' Knowledge:** Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

- **The Data Broker Industry is Complex, with Multiple Layers of Data Brokers Providing Data to Each Other:** Data brokers provide data not only to end-users, but also to other data brokers. The nine data brokers studied obtain most of their data from other data brokers rather than directly from an original source. Some of those data brokers may in turn have obtained the information from other data brokers. Seven of the nine data brokers in the Commission's study provide data to each other. Accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers.

- **Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer:** Data brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction. Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each

month to its databases. Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer.

- **Data Brokers Combine and Analyze Data About Consumers to Make Inferences About Them, Including Potentially Sensitive Inferences:** Data brokers infer consumer interests from the data that they collect. They use those interests, along with other information, to place consumers in categories. Some categories may seem innocuous such as "Dog Owner," "Winter Activity Enthusiast," or "Mail Order Responder." Potentially sensitive categories include those that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African Americans with low incomes. Other potentially sensitive categories highlight a consumer's age such as "Rural Everlasting," which includes single men and women over the age of 66 with "low educational attainment and low net worths," while "Married Sophisticates" includes thirty-something couples in the "upper-middle class . . . with no children." Yet other potentially sensitive categories highlight certain health-related topics or conditions, such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus."

- **Data Brokers Combine Online and Offline Data to Market to Consumers Online:** Data brokers rely on websites with registration features and cookies to find consumers online and target Internet advertisements to them based on their offline activities. Once a data broker locates a consumer online and places a cookie on the consumer's browser, the data broker's client can advertise to that consumer across the Internet for as long as the cookie stays on the consumer's browser. Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities. Some data brokers are using similar technology to serve targeted advertisements to consumers on mobile devices.

2. Benefits and Risks

- **Consumers Benefit from Many of the Purposes for Which Data Brokers Collect and Use Data:** Data broker products help to prevent fraud, improve product offerings, and deliver tailored advertisements to consumers. Risk mitigation products provide significant benefits to consumers by, for example, helping prevent fraudsters from impersonating unsuspecting consumers. Marketing products benefit consumers by allowing them to more easily find and enjoy the goods and services they need and prefer. In addition, consumers benefit from increased and innovative product offerings fueled

by increased competition from small businesses that are able to connect with consumers they may not have otherwise been able to reach. Similarly, people search products allow individuals to connect with old classmates, neighbors, and friends.

- **At the Same Time, Many of the Purposes for Which Data Brokers Collect and Use Data Pose Risks to Consumers:** There are a number of potential risks to consumers from data brokers' collection and use of consumer data. For example, if a consumer is denied the ability to conclude a transaction based on an error in a risk mitigation product, the consumer can be harmed without knowing why. In such cases, the consumer is not only denied the immediate benefit, but also cannot take steps to prevent the problem from recurring. Similarly, the scoring processes used in some marketing products are not transparent to consumers. This means that consumers are unable to take actions that might mitigate the negative effects of lower scores, such as being limited to ads for subprime credit or receiving different levels of service from companies. As to other marketing products, they may facilitate the sending of advertisements about health, ethnicity, or financial products, which some consumers may find troubling and which could undermine their trust in the marketplace. Moreover, marketers could even use the seemingly innocuous inferences about consumers in ways that raise concerns. For example, while a data broker could infer that a consumer belongs in a data segment for "Biker Enthusiasts," which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using that same segment might infer that the consumer engages in risky behavior. Similarly, while data brokers have a data category for "Diabetes Interest" that a manufacturer of sugar-free products could use to offer product discounts, an insurance company could use that same category to classify a consumer as higher risk. Finally, people search products can be used to facilitate harassment, or even stalking, and may expose domestic violence victims, law enforcement officers, prosecutors, public officials, or other individuals to retaliation or other harm.

- **Storing Data About Consumers Indefinitely May Create Security Risks:** Some of the data brokers store all data indefinitely, even if it is later updated, unless otherwise prohibited by contract. For some products, these data brokers report that they need to keep older data. For example, they explain that even if a consumer's address is outdated, it is important to keep the consumer's address history in order to verify the consumer's identity. For other products, however, retention of older data may not be necessary. An older address may be less relevant to deliver marketing to a consumer. Although stored data may be useful for future business purposes, the risk of keeping the data may outweigh the benefits. For example, identity thieves and other unscrupulous actors may

be attracted to the collection of consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials.

3. Consumer Choice

- **To the Extent Data Brokers Offer Consumers Choices About Their Data, the Choices are Largely Invisible and Incomplete:** Some data brokers provide consumers with choices about their data, but because data brokers are not consumer-facing, consumers may not know where to go to exercise any choices that may be offered. In addition, the data brokers' opt outs do not clearly convey whether the consumer can exercise a choice to opt out of all uses of consumer data, and therefore, consumers may find the opt outs confusing. As a result, even those consumers who know who the data brokers are, find their websites, and take the time to find the opt out and use it may still not know its limitations. For marketing products, the extent of consumers' choices over their data is not clear. For risk mitigation products, many data brokers do not provide consumers with access to their data or the ability to correct inaccurate data.

B. Legislative Recommendations

Many of the above findings point to a fundamental lack of transparency about data broker industry practices. Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered quite sensitive; and share the information with clients in a range of industries. Much of this activity takes place without consumers' knowledge. In light of these findings, the Commission unanimously recommends that Congress should consider enacting legislation that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities.

The specific legislative recommendations detailed below build on the Commission's work for the last two decades to improve transparency and choice in the data broker industry. Indeed, despite the Commission's call for greater transparency in the 1990s, the IRSG self-regulatory experiment to improve transparency of data broker practices was short-lived. Since then, data broker practices have grown dramatically in breadth and depth, as data brokers have the ability to collect information from more sources, including consumers' online activities; analyze it through new and emerging algorithms and business models; and store the information indefinitely due to dwindling storage costs. Despite the Commission's recommendations, lack of transparency and choice remain significant issues in this industry.

The specific legislative recommendations discussed below reflect high-level principles drawn from the findings of this study, the Commission's previous work in this area, and the ongoing public debate about

data brokers. Among other things, the recommendations borrow from the Commission's best practice and legislative recommendations regarding data brokers in its 2012 Privacy Report; self-regulatory developments among industry members;[79] and the Commission's extensive enforcement experience with data broker practices. For example, the Commission's case against ChoicePoint, described above, underscores the importance of employing reasonable and appropriate measures to screen clients before sharing consumers' information in order to secure the consumer information retained by the data broker.[80] The Commission's case against data broker U.S. Search addressed the importance of disclosing any limitations on opt-outs.[81]

The Commission has organized its legislative recommendations by product type. In offering these high-level recommendations, the Commission recognizes that it will be important to weigh the costs and benefits of more concrete legislative proposals as they are developed.[82]

1. Marketing Products

The Commission recommends that Congress consider legislation requiring data brokers to give consumers (1) access to their data and (2) the ability to opt out of having it shared for marketing purposes.[83] Currently, consumers do not have meaningful information about which data brokers may have their data, nor do consumers have meaningful information about where they can access their data or how they can exercise any opt-out rights that data brokers may already provide.

To enable consumers to efficiently avail themselves of these rights, legislation could also 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.[84] This

79 *See* AboutTheData, https://www.aboutthedata.com/ (last visited May 19, 2014).

80 United States v. ChoicePoint, No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009) (Supplemental Stipulated J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/10/091019choicepointstiporder.pdf; United States v. ChoicePoint, Inc., No. 1:06-CV-0198-JTC (N.D. Ga. Feb. 15, 2006) (Stipulated Final J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

81 US Search, Inc., No. C-4317, at 6–7 (F.T.C. Mar. 14, 2011) (Decision and Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110325ussearchdo.pdf.

82 The following legislative and best practice recommendations reflect the consensus of a majority of the Commission. To the extent that particular Commissioners have different viewpoints on a particular legislative or best practice recommendation, those viewpoints can be found in footnotes below or in a separate statement. Commissioner McSweeny did not participate in the Commission vote on this report.

83 As noted above, data brokers often refer to such an opt out as data "suppression." *See* Section VII.A. and *supra* note 54.

84 *See* Privacy Report, *supra* note 9, at 69–70.

approach would enable consumers to visit a single site to ascertain what kinds of information data brokers have about them and how to exercise opt-out choices.[85]

Some industry members have expressed concern that such a centralized portal would be unwieldy, given the sheer number of data brokers in the marketplace and the fact that consumers may be overwhelmed by the breadth of information. To address this concern, in creating such a portal, Congress could consider limiting the portal to a number of the largest data brokers (fifty, for example, or other number deemed appropriate).[86] This approach is similar to that contained in the FCRA, which places CRAs in different tiers. All CRAs are subject to some requirements; other requirements apply only to "nationwide specialty CRAs;" and still other requirements apply only to "nationwide CRAs." The FCRA requires the "nationwide CRAs" to create a centralized website which grants consumers the ability to access their free annual credit reports.[87]

The Commission recommends that Congress consider requiring data brokers to provide consumers with access to their data, including any sensitive data, at a reasonable level of detail. Because data brokers create and manipulate thousands of data elements and segments, it would be very difficult for consumers to interpret and digest an access tool that gave them access to every category of data a data broker has about them. Despite these challenges, Congress should consider requiring data brokers to provide enough detail that a consumer can see the breadth of categories the data broker has about them, including any sensitive data.

Allowing consumers the ability to exercise control over the use of sensitive information is particularly important. There appears to be widespread agreement on certain core sensitive categories of data—such as whether a consumer has AIDS, diabetes, or depression—while the sensitivity of other information may lie in the "eye of the beholder." For categories that some consumers might find sensitive and others may not (e.g., visually impaired, balding, overweight), having access to this data, along with the ability to suppress the use

85 Commissioner Wright agrees that Congress should consider legislation that would provide for consumer access to the information collected by data brokers. However, he does not believe that at this time there is enough evidence that the benefits to consumers of requiring data brokers to provide them with the ability to opt out of the sharing of all consumer information for marketing purposes outweighs the costs of imposing such a restriction. Finally, although the concept of a centralized portal to provide consumers with information about the practices of data brokers may be useful in theory, he believes that the Commission should engage in a rigorous study of consumer preferences sufficient to establish that consumers would likely benefit from such a portal prior to making such a recommendation.

86 Because there may be many ways to define the universe of "large data brokers," it may be appropriate for any legislation that addresses this issue to include a rulemaking, similar to the rulemakings the Consumer Financial Protection Bureau undertook to determine the "larger participants" that would be subject to its examination authority. See Section 1024 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5514(a)(1)(B) (2012).

87 *See* 15 U.S.C. § 1681j (2012); see also 16 C.F.R. § 1022.136 (2012); Annual Credit Report, http://www.annualcreditreport.com/ (last visited May 19, 2014).

of it for marketing, will improve the transparency of data broker practices and allow consumers to control uses of the data about which they care the most.[88]

In addition, to further enhance transparency, the Commission recommends that Congress consider legislation requiring data brokers to clearly disclose to consumers (e.g., on their website) that they not only use the raw data that they obtain from their sources, such as a person's name, address, age, and income range, but that they also derive certain inferences from the data. For example, the data broker may explain that it infers a consumer's interests from the consumer's licenses, newspaper and magazine subscriptions, websites visited, or previous purchases.[89] Congress should also consider requiring data brokers to clearly disclose the names and/or categories of their data sources, so that consumers are better able to determine if, for example, they need to correct their data with an original public record source.[90] Of course, any legislation in this area should weigh the potential security risks of providing access to individual consumer data and any potential methods for mitigating such risks.

Given the current invisibility of data brokers, the question remains: If these access and opt-out tools were to exist and be available to consumers through a centralized mechanism, how would a consumer learn about them? One way legislation could increase the visibility of the data broker industry and the access and opt-out tools they offer is to require that consumer-facing sources provide a prominent notice to consumers that they share consumer data with data brokers and give consumers choices, such as the ability to opt out of sharing their information with data brokers. Congress should also consider imposing important protections for sensitive information, such as certain health information, by requiring that consumer-facing sources obtain consumers' affirmative express consent before collecting and sharing such information with data brokers. Finally, Congress should consider requiring that consumer-facing sources provide the names of the data brokers to which they provide data, along with information or links to the centralized mechanism with its description of the access and opt-out rights offered by these data brokers.[91] Providing such notice at the

88 Commissioner Wright believes that in enacting statutes such as the Fair Credit Reporting Act, Congress undertook efforts to balance the benefits of information collection and sharing (fair and accurate credit reporting is beneficial to both businesses and consumers) against the costs of such information collection and sharing (potential risks to confidentiality, accuracy, relevancy, and appropriate use). In doing so, Congress carefully articulated the types of information to be protected, limited the use and access to such information, and provided certain consumer protections relating to the accuracy of and the ability to dispute and correct such information. In the instant case, Commissioner Wright is wary of extending FCRA-like coverage to other uses and categories of information without first performing a more robust balancing of the benefits and costs associated with imposing these requirements.

89 This recommendation is not intended to require data brokers to disclose their proprietary algorithms.

90 For example, Acxiom has released a tool that provides consumers with access to information about the categories of sources from whom the company obtains its data. *See* AboutTheData, *supra* notes 76 & 79.

91 In addition, Chairwoman Ramirez and Commissioner Brill believe that data brokers should take reasonable steps, such as through contractual provisions with their immediate data source, to ensure that the consumer data they obtain was procured by the original source—such as a retailer—with notice and choice, including express affirmative consent for sensitive data, in the manner outlined above. Accordingly, they recommend that Congress consider including a provision to this effect in legislation. In the absence of such a legal requirement, they believe that data brokers should, as a best practice, contractually require their immediate sources to take reasonable steps to ensure, to the extent practicable, that the original source of data had provided notice and choice to consumers in the manner described above.

source could give consumers a timely opportunity to learn that their data is shared with data brokers and to exercise choices about such sharing.[92]

The Commission recognizes the reality that many consumers will not seek access to the data maintained by the data brokers and that those who do may not understand the nuances of how their data is used. However, the legislative recommendations in this section will do more than provide transparency to individual consumers. They also will promote accountability by allowing other key stakeholders—including regulators, policymakers, academics, industry, and consumer advocates—to assess whether data brokers are clearly and accurately describing their practices to consumers.

2. Risk Mitigation Products

The Commission recommends that Congress consider legislation that would provide consumers with transparency when a company uses a risk mitigation product that limits a consumer's ability to complete a transaction. Such legislation could address scenarios that the FCRA may not cover. Consider the example of John Doe applying for a new mobile telephone contract. If a data broker's product is used to assess John Doe's ability to pay his bills on time, the FCRA would likely apply, because its obligations are generally triggered when consumers are denied credit, employment, housing, insurance, government benefits, or the ability to engage in a transaction that they initiated—such as an application for a mobile telephone contract. The Commission aggressively enforces the FCRA in connection with these and other uses.[93]

If, however, the mobile telephone company uses a risk mitigation product only to confirm John Doe's identity—i.e., to determine whether John Doe is in fact John Doe and not an identity thief—the FCRA may not apply. Despite the differing objectives, the ultimate result could be the same—John Doe cannot obtain a mobile telephone contract.[94] In essence, he may be prevented from completing a transaction without knowing why.[95] Congress should consider enacting legislation to address this scenario. Congress should consider requiring that, if a risk mitigation product adversely impacts a consumer's ability to

92 These recommendations complement the Commission's previous recommendations with respect to consumer-facing data sources from the 2012 Privacy Report. *See* Privacy Report, *supra* note 9, at 35, 47–50.

93 *FTC Statement on Data Brokers, supra* note 3, at 4 ("The Commission maintains an aggressive FCRA enforcement program. To date, it has brought almost 100 cases and obtained in excess of $30 million in civil penalties.").

94 The determination of whether the FCRA applies does not turn on whether the data broker labels a product as a "risk mitigation" product. There may be instances in which a product that is marketed as a risk mitigation product may be covered by the FCRA because, for example, it is used to determine creditworthiness. Whether the FCRA applies to particular uses of consumer data depends on the specific facts involved, and the FTC will make these determinations on a case-by-case basis.

95 The Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products. In a different context, a recent Commission Report assessed the accuracy of consumer information in credit reports and found that 5.2% of consumers had errors on at least one of their three major credit reports that could lead to them paying more for products such as auto loans and insurance. *See* Fed. Trade Comm'n, Section 319 of the Fair and Accurate Credit Transactions Act of 2003: Fifth Interim Federal Trade Commission Report to Congress Concerning the Accuracy of Information in Credit Reports 47 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf.

complete a transaction or obtain a benefit, the consumer-facing company should identify the data brokers upon whose data the company relied. These data brokers should in turn give consumers the right to access the information used and correct any erroneous information, as appropriate. One of the data brokers in our study already implements a similar approach for its risk mitigation products. The required level of transparency, access, and correction should be tied to the significance of the benefit or transaction in question.[96]

It would likely be impractical for data brokers whose risk mitigation products rely on hundreds or more data elements to provide access to every data element used to develop the products. However, data brokers could provide access to the results generated by the products, any explanatory codes associated with the results, the range of possible results, and a description of how the results are developed. This information would help consumers dispute or correct any errors. At the same time, one would not want an unscrupulous individual to be able to "correct" his or her own truthful data. For this reason, Congress should consider how to enable consumer access while preserving the accuracy and security of such data.

3. People Search Products

Finally, the Commission unanimously recommends that Congress consider legislation requiring data brokers offering people search products to: (1) allow consumers to access their own information; (2) allow consumers to opt out of the use of this information; (3) clearly disclose to consumers the data brokers' sources of information, so that, if possible, the consumer can correct his or her information at the source; and (4) clearly disclose any limitations of the opt out, such as the fact that close matches of an individual's name may continue to appear in search results.[97]

C. Best Practice Recommendations

More generally, the Commission continues to call on data brokers in all product categories to adopt the principles contained in the Privacy Report, to the extent they have not already done so in the two years since the Commission issued its report. In addition to the specific recommendations described above, they should also practice privacy by design, which includes considering privacy issues at every stage of product development.

96 Commissioner Wright believes that this recommendation is premature because there is no evidence about the existence or scope of this hypothetical problem. As noted in *supra* note 95, the Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products.

97 *See* US Search, Inc., No. C-4317, at 6–7 (F.T.C. Mar. 14, 2011) (Decision and Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110325ussearchdo.pdf (alleging deception where a company's "Privacy Lock" service would not prevent a consumer's name and other information from appearing in many instances, including as an associate on another person's profile, in a "reverse search," or if the consumer changed addresses, thereby generating a new record).

As part of privacy by design, data brokers should strive to assess their collection practices and, to the extent practical, collect only the data they need and properly dispose of the data as it becomes less useful. This is particularly important in light of companies' increased ability to collect, aggregate, and match consumer data and to develop secondary uses for the data in ways that consumers could never have contemplated when they provided the information. Sound data collection and disposal practices also reinforce data security, as collecting and storing large amounts of data not only increases the risk of a data breach or other unauthorized access but also increases the potential harm that could be caused.[98] For example, identity thieves and other unscrupulous actors may be attracted to detailed consumer profiles maintained by data brokers[99] that do not dispose of obsolete data, as this data could give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, answers to challenge questions, or other authentication credentials.

Data brokers also should implement better measures to refrain from collecting information from children and teens, particularly in marketing products. As to children under 13, COPPA already requires certain online services to refrain from collecting personal information from this age group without parental consent; the principles underlying that legislation could apply equally to information collected offline from children.[100] As to teens, the Commission previously has noted that they often lack the judgment to appreciate the long-term consequences of, for example, posting data on the Internet.[101] And as noted above, it appears that some of the data brokers themselves have policies or have stated that they do not use teens' data in their marketing products; yet they may not check data from their sources to ascertain whether it contains such data. Data brokers providing data for marketing products should take further reasonable steps to avoid collecting and using teens' and children's data.

Finally, the Commission recommends that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes.[102] For example, while the data segment of "Smoker in Household" could be used to market a new air filter, a downstream entity also could use the segment to suggest that a person is a poor credit or

98 *See* Privacy Report, *supra* note 9, at 24, 26–29. Commissioner Ohlhausen does not support a strict data minimization requirement.

99 *Cf.* United States v. ChoicePoint, Inc., No. 1:06-CV-0198-JTC (N.D. Ga. Feb. 15, 2006) (Stipulated Final J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

100 For example, under § 312.7 of the COPPA Rule, an operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. 16 C.F.R. § 312.7.

101 *See* Privacy Report, *supra* note 9, at 59–60.

102 On September 15, 2014, the Commission will examine the potential effects of "Big Data" on American consumers, at a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?." *See* 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. *See also* Exec. Office of the President, Big Data: Seizing Opportunities, Preserving Values 51–53 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (discussing the potential for big data uses to result in discrimination).

insurance risk, or an unsuitable candidate for employment or admission to a university. This would be especially pernicious if the segment included a high concentration of minorities. Of course, the use of race, color, religion, and certain other categories to make credit, insurance, and employment decisions is already against the law,[103] but data brokers should help ensure that the information does not unintentionally go to unscrupulous entities[104] that would be likely to use it for unlawful discriminatory purposes.[105] Similarly, data brokers should conduct due diligence to ensure that data that they intend for marketing or risk mitigation purposes is not used to deny consumers credit, insurance, employment, or the like.[106]

Some of the data brokers are already contractually limiting the purposes for which their clients can use their data. A subset of these data brokers goes further, by "seeding" data[107] or auditing their clients to ascertain that it is not being used for a contractually prohibited purpose. The Commission's recommendations on this issue seek to build on these best practices.[108]

103 *See, e.g.*, *Equal Credit Opportunity Act*, 15 U.S.C. § 1691–1691f (2012) (prohibiting discrimination in credit decisions on the basis of race, color, religion, national origin, sex, marital status, age, and receipt of public assistance).

104 This recommendation is analogous to current FCRA requirements. *See* 15 U.S.C. § 1681e. It is also analogous to the relief required in the consent decree resulting from the Commission's *ChoicePoint* case, in which the Commission alleged a data broker had violated the FCRA by failing to employ reasonable and appropriate measures to secure the personal information it collected for sale to its subscribers, including reasonable policies and procedures to verify or authenticate the identities and qualifications of prospective subscribers, thereby enabling downstream illegal uses of consumers' data. *See* Complaint at 7–8, United States v. ChoicePoint, No. 1:06-CV-0198-JTC (N.D. Ga. Feb. 16, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf. Notably, because some of ChoicePoint's activities were not FCRA-covered, the Commission alleged that ChoicePoint's failure to implement these policies and procedures was also an unfair practice under Section 5 of the FTC Act. *Id.* at 9. Under the consent decree, ChoicePoint must, among other things, establish and maintain reasonable procedures to ensure that consumer reports are provided only to those with a permissible purpose and verify the identity of businesses that apply to receive consumer reports, including making site visits to certain business premises and auditing subscribers' use of consumer reports. *See* United States v. ChoicePoint, Inc., No. 1:06-CV-0198-JTC (N.D. Ga. Feb. 15, 2006) (Stipulated Final J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

105 Commissioner Wright believes that to the extent that information is being used for unlawful discriminatory purposes, the Commission's law enforcement authority is the appropriate vehicle to address this problem. He also notes the Commission plans to examine issues related to "Big Data" at a September workshop. *See supra* note 102. Before imposing additional obligations on data brokers to conduct due diligence, he would like to see evidence about the existence, nature, and scope of any such problematic uses.

106 If the data broker's activities do not meet the definition of a "consumer reporting agency," as defined by the FCRA, these uses of the data would not trigger FCRA protections.

107 Some data brokers systematically add unique dummy data, or "seed" data, into their databases to monitor how this data is being used by their partners, resellers, or end clients.

108 Chairwoman Ramirez and Commissioner Brill believe that legislation—rather than simply a best practice recommendation—is warranted to help ensure that consumers are protected from unlawful uses of data supplied by data brokers.

IX. CONCLUSION

In the nearly two decades since the Commission first began to examine data brokers, little progress has been made to improve transparency and choice. While data brokers provide important benefits to consumers, and some data brokers have taken steps to improve their privacy practices, overall transparency in this industry continues to be lacking. And with the emergence of new sources of information, improvements in analytics methods, and the availability of more granular information about individual consumers, the need for consumer protections in this area has never been greater.

This report attempts to provide a window into data brokers' collection and use of consumer information and makes recommendations to enhance transparency and consumer control. It also raises concerns about the collection of sensitive data about consumers and the development of labels and categories that could be used to target and potentially discriminate against consumers. The findings and recommendations in this report are intended to be part of an ongoing dialogue, and the Commission welcomes further input and information on these issues. The Commission will continue to work with industry, consumer groups, and lawmakers to further the goals of increased transparency and consumer control.

APPENDIX A:
Text of the Model Order

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen

File No. P125404

ORDER TO FILE SPECIAL REPORT

Pursuant to a resolution of the Federal Trade Commission ("FTC" or "the Commission") dated December 14, 2012, titled "Resolution Directing Use of Compulsory Process to Collect Information Regarding Data Brokers," a copy of which is enclosed, **[COMPANY NAME]**, hereinafter referred to as the "Company," is ordered to file with the Commission, no later than **February 1, 2013**, a Special Report containing the information and documents specified herein.

The information provided in the Special Report will assist the Commission in compiling a study of data broker industry information collection and use activities.

The Special Report must restate each item of this Order with which the corresponding answer is identified. Your report is required to be subscribed and sworn by an official of the Company who has prepared or supervised the preparation of the report from books, records, correspondence, and other data and material in your possession. If any question cannot be answered fully, give the information that is available and explain in what respects and why the answer is incomplete. The Special Report and all accompanying documentary responses must be Bates-stamped.

Confidential or privileged commercial or financial information will be reported by the Commission on an aggregate or anonymous basis, consistent with Sections 6(f) and 21(d) of the FTC Act. Individual submissions responsive to this Order that are marked "confidential" will not be disclosed without first giving the Company ten (10) days notice of the Commission's intention to do so, except as provided in Sections 6(f) and 21 of the FTC Act.

Specifications

Please provide the following information, documents and items, consistent with the definitions, instructions, and formatting requirements contained in Attachment A:

1. **Identification of Report Author:** Identify by full name, business address, telephone number, and official capacity the person(s) who has prepared or supervised the preparation of the Company's response to this Order and describe in detail the steps taken by the Company to respond to this Order. For instructions pertaining to document (written and electronic) and information preservation, identify the person who gave the instructions, describe the content of any oral instructions, provide copies of any written or electronic instructions, and identify the person(s) to whom the instructions were given. For each specification, identify the individual(s) who assisted in preparation of the response. Provide a list of the persons (identified by name and corporate title or job description) whose files were searched and identify the person who conducted the search.

2. **Company Information:**

    A. State the Company's complete legal name and all other names under which it has done business, its corporate mailing address, all addresses from which it does or has done business, and the dates and states of its incorporation.

    B. Describe the Company's corporate structure, and state the names of all parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which it exercises supervision or control. For each such entity, describe the nature of its relationship to the Company.

    C. Identify each individual or entity having an ownership interest in the Company, as well as their individual ownership stakes and their positions and responsibilities within the Company.

3. **Products and Services:**

    A. Provide a list and description as to the nature and purpose of all the products and services (both online and offline) that the Company offers or sells that use personal data. Include a separate description of each product or service identified; and for each product or service, describe with specificity each type of personal data that is used in or by the product or service; and identify and describe with specificity:

(1) the source(s) of each such type of personal data, including whether the source is a government agency or office;

(2) the procedures or means by which each such type of personal data is collected, generated, or derived, including, but not limited to, cookies, a user's direct textual input, a user's behavior on the Company's website, a user's behavior on other websites, social media, a user's mobile use and activity, or other online or offline sources;

(3) for each such type of personal data, whether the Company acquires the consent, permission, or approval of consumers before obtaining, collecting, generating, deriving, disseminating, storing, or causing to be stored the personal data of said consumers. As part of your response, describe in detail how the Company obtains the consent, permission, or approval of said consumers;

(4) the frequency with which each such type of personal data is updated;

(5) the extent to which and reasons why the availability of each such type of personal data differs depending upon the purchaser;

(6) whether the Company provides each such type of personal data to users in the form in which it is acquired or whether the Company changes the form or content of such type of personal data in any way, and for the latter describe each and every way in which the Company changes the form or content of each such type of personal data and the methodology employed to effect such change;

(7) whether each such type of personal data is aggregated, anonymized, or de-identified and describe the process used to do so;

(8) whether each such type of personal data includes information from or about children or teenagers. As part of your response, describe in detail whether the Company distinguishes personal data about children ages 12 and under from personal data about teenagers ages 13 through 17 and how the collection and provision of this data differs.

B. State whether the Company monitors, audits, or evaluates the accuracy of personal data contained in each product or service identified in response to 3.A. If it does, provide a step-by-step explanation of how the Company monitors, audits, or evaluates the accuracy of such personal data, and describe the results from the Company's audits, evaluations, and monitoring efforts, including the accuracy rates for the personal data contained in each product or service. As part of your response, describe in detail:

(1) the Company's policies, practices, and procedures relating to the monitoring, auditing, or evaluation of the accuracy of personal data contained in each product or service;

(2) the Company's search and retrieval logic for matching its records with particular consumers; and

(3) the Company's matching logic (i.e., evaluations regarding the effectiveness of the information submitted by clients and/or used by the Company about consumers in retrieving results related to the correct consumer);

C. For each product or service identified in response to 3.A., indicate (1) the number of such products or services sold annually, and (2) the Company's annual gross revenues attributable to each such product or service.

4. **Other Collection of Data:**

A. Identify each type of personal data the Company has obtained, collected, generated, derived, disseminated, stored, or caused to be stored that is not currently used in or by a product or service identified in your response to 3.A., and describe with specificity:

(1) the reason(s) why each such type of personal data is not currently used in or by a product or service and any plans for future use;

(2) for each such type of personal data that was previously used in a product or service, identify (i) the name of the product(s) or service(s) that used the personal data, (ii) the number of such products or services sold annually, (iii) the Company's annual gross revenues attributable to each such product or service, (iv) the types of customers (e.g., individual consumers, retailers, ad networks, etc.) to which the Company provided each product or service, (v) the percentage of the product's or service's revenue contributed by each type of customer, and (vi) the names and contact information of the product's or service's 25 largest

customers (25 entities who purchased the greatest unit and dollar amounts of each product or service) for each type of customer except individual consumers;

(3) the source of each such type of personal data, including whether the source is a government agency or office;

(4) the procedures or means by which each such type of personal data is or was collected, generated, or derived, including, but not limited to, cookies, a user's direct textual input, a user's behavior on the Company's website, a user's behavior on other websites, social media, a user's mobile use and activity, or other online or offline sources;

(5) for each such type of personal data, whether the Company acquires or acquired the consent, permission, or approval of consumers before obtaining, collecting, generating, deriving, disseminating, storing, or causing to be stored the data of said consumers. As part of your response, describe in detail how the Company obtains the consent, permission, or approval of said consumers;

(6) the frequency in which each such type of personal data is or was updated;

(7) the extent to which and reasons why the availability of each such type of personal data differs or differed depending upon the purchaser;

(8) each specific purpose or manner in which the Company anticipates or anticipated that each such type of personal data would or could be used by its users or customers and any limitations the Company places or placed on the use of each such type of personal data;

(9) whether the Company provides or provided each such type of personal data to users in the form in which it is acquired or whether the Company changes or changed the form or content of such type of personal data in any way, and for the latter describe each and every way in which the Company changes or changed the form or content of each such type of personal data and the methodology employed to effect such change;

(10) whether each such type of personal data is or was aggregated, anonymized, or de-identified and describe the process used to do so;

(11) whether each such type of personal data includes or included information from or about children or teenagers. As part of your response, describe in detail whether the Company distinguishes or distinguished personal data about children ages 12 and under from personal data about teenagers ages 13 through 17 and how the collection and provision of this data differs or differed.

B. State whether the Company monitors, audits, or evaluates the accuracy of personal data contained in each product or service identified in response to 4.A., either presently or previously. If it does, provide a step-by-step explanation of how the Company monitors, audits, or evaluates the accuracy of such personal data, and describe the results from the Company's audits, evaluations, and monitoring efforts, including the accuracy rates for the personal data contained in each product or service. As part of your response, describe in detail:

(1) the Company's policies, practices, and procedures relating to the monitoring, auditing, or evaluation of the accuracy of personal data contained in each product or service;

(2) the Company's search and retrieval logic for matching its records with particular consumers; and

(3) the Company's matching logic (i.e., evaluations regarding the effectiveness of the information submitted by clients and/or used by the Company about consumers in retrieving results related to the correct consumer);

5. **Customers**:

A. For each product or service identified in your response to 3.A., identify the types of customers (e.g., individual consumers, retailers, ad networks, etc.) to which the Company provides each product or service, the percentage of the product's or service's revenue contributed by each type of customer, and the names and contact information of the product's or service's 25 largest customers (25 entities who purchased the greatest unit and dollar amounts of each product or service) for each type of customer except individual consumers. As part of your response, describe in detail:

(1) the method(s) by which the Company provides each product or service;

(2) the fees associated with each product or service;

(3) a step-by-step explanation of how the Company's customers access

the Company's products and services and the flow of personal data from the initial request made to the Company to the furnishing of personal data to the customer;

(4) all of the purposes, and how the Company determines the purposes, for which the Company's customers use personal data provided by the Company, including but not limited to marketing, background screening, resale, or fraud detection purposes;

(5) how the Company evaluates its customers (e.g., whether the Company evaluates whether a customer is a legitimate business entity and its data security measures) at the time of purchase; and

(6) whether the Company reviews, monitors, audits, or evaluates how its customers use personal data post-purchase and the nature, timing, results, and actions taken as the result of these reviews, audits, or evaluations.

B. For each product or service identified in your response to 3.A., describe in detail any prohibitions or restrictions (e.g., contractual, technological) the Company communicates or enforces against its customers on the sale or use of such product or service. As part of your response, explain:

(1) whether the Company's contracts, agreements, and terms and conditions of use between the Company and any user of any of the Company's products or services enumerate such prohibitions and restrictions. Provide contracts, agreements, and terms and conditions of use for the Company's three largest customers for each type of customer identified in your response to 5.A. and four other examples representing the range of contracts, agreements, and terms and conditions of use for each type of customer identified in your response to 5.A.;

(2) how the Company monitors compliance with such prohibitions or restrictions; and

(3) whether the Company has ever taken any action against a customer to enforce such prohibitions or restrictions and, if so, a description of those actions.

6. **Consumers:**

A. State whether consumers are able to access personal data about them that is held by the Company. If consumers are not able to access their personal data, state the Company's rationale for not providing such access. If consumers are able to access their personal data, describe in detail how consumers access this personal data, including but not limited to:

(1) a step-by-step explanation of how consumers access such personal data;

(2) the types of personal data that consumers can and cannot access;

(3) the terms and conditions for accessing personal data, including any limitations on the frequency of access;

(4) how the Company notifies consumers of their right to access this personal data and the contents of the notice;

(5) the types of personal information consumers are required to provide to verify their identities prior to accessing their personal data, and how the Company utilizes this verification information;

(6) the number of consumers that have requested access to their personal data on an annual basis and the Company's response by category (i.e., number of consumers provided access, number of consumers denied access, reasons for denial, etc.);

(7) the date on which the Company first began to give consumers access to personal data; and

(8) the average and maximum length of time before an access request is implemented, and the factors that determine the length of time before access is provided.

B. State whether consumers are able to correct personal data that is held by the Company. If consumers are not able to correct their personal data, state the Company's rationale for not allowing such corrections. If consumers are able to correct their personal data, describe in detail how consumers correct their personal data, including but not limited to:

(1) a step-by-step explanation of how consumers correct such personal data;

(2) the types of personal data that consumers can and cannot correct;

(3) the terms and conditions for correcting personal data, including the Company's efforts to prevent the reappearance of inaccurate data;

(4) how the Company notifies consumers of their right to correct this personal data and the contents of the notice;

(5) the types of personal information consumers are required to provide to verify their identities before correcting their personal data, and how the Company utilizes this verification information;

(6) the number of consumers that have requested a correction to their personal data on an annual basis and the Company's response by category (i.e., number of corrections, number not corrected, reasons for not correcting, etc.);

(7) the date on which the Company first began to give consumers the ability to correct their personal data; and

(8) the average and maximum length of time before a correction request is implemented, and the factors that determine the length of time before the correction takes effect.

C. State whether consumers are able to opt out of the collection, use, or sharing of their personal data. If consumers are not able to opt out, state the Company's rationale for not allowing consumers to opt out. If consumers are able to opt out, describe in detail the Company's opt out procedures, including but not limited to:

(1) a step-by-step explanation of how consumers opt out;

(2) the specific products, services, or search results to which the opt out applies and does not apply;

(3) the terms and conditions for opting out;

(4) the technologies utilized to effectuate the opt out;

(5) how the Company notifies consumers of their right to opt out and the contents of the notice;

(6) the types of personal information consumers are required to provide to verify their identities before opting out, and how the Company utilizes this verification information;

(7) the number of consumers that have requested to opt out on an annual basis and the Company's response by category (i.e., number of opt outs provided, number of opt outs denied, reasons for denial, etc.);

(8) the date on which the Company first began to give consumers the ability to opt out; and

(9) the average and maximum length of time before an opt out request is implemented, the factors that determine the length of time before the opt out takes effect, and the period of time the opt out remains in effect.

D. State whether consumers are able to have the Company delete their personal data from the Company's database(s). If consumers are not able to delete their personal data, state the Company's rationale for not allowing such deletions. If consumers are able to delete their personal data, describe in detail how consumers delete their personal data, including but not limited to:

(1) a step-by-step explanation of how consumers delete such personal data;

(2) the types of personal data that consumers can and cannot delete;

(3) the terms and conditions for deleting personal data, including the Company's efforts to prevent reinsertion of the data;

(4) how the Company notifies consumers of their right to delete this personal data and the contents of the notice;

(5) the types of personal information consumers are required to provide to verify their identities before deleting their personal data, and how the Company utilizes this verification information;

(6) the number of consumers that have requested to delete their personal data on an annual basis and the Company's response by category (i.e., number of deletions provided, number of deletions denied, reasons for denial, etc.);

(7) the date on which the Company first began to give consumers the ability to delete their personal data; and

(8) the average and maximum length of time before a deletion request is implemented, and the factors that determine the length of time before the deletion takes effect.

E. State whether the Company charges consumers a fee for accessing, correcting, opting out, or deleting their personal data from the Company's database(s). As part of your response, describe in detail:

(1) the amount the Company charges consumers to access, correct, delete, or opt out; and

(2) the total revenue earned annually by the Company through such fees.

F. In your responses to 6.A-E., describe each and every way in which the Company's procedures relating to children and teenagers is different from the Company's procedures relating to adults.

7. **Policies:**

A. State the methods by which the Company provides notice to consumers about the Company's personal data collection, use, or sharing practices. Provide representative samples of any notices or disclosures provided to consumers in connection with the products and services identified in response to 3.A.

B. State whether the Company has (or had) any written policies or statements regarding the collection, disclosure, and use of personal data, including any policies and statements relating to the privacy or security of such data. Provide a copy of each such policy or statement, indicating for each the date on which it became effective and, if applicable, all means by which it was distributed or made available. If the policies changed at any time, please so state and describe the nature of the change and its effective time period.

C. Identify the names and titles of the individuals at the Company who are responsible for developing and implementing any policies described in your responses to each specification.

8. **Promotional Materials and Advertisements:**

A. Provide representative samples of each type of advertisement or promotional material the Company has disseminated referring or relating to the products and services identified in response to 3.A. or the personal data identified in response to 4.A., including but not limited to websites, emails, advertisements, and brochures. For each advertisement or promotional material provided, state the beginning and ending dates of dissemination, and the dates, times, and locations the ads were disseminated. For print ads and press releases, identify every publication, date, and community for dissemination; for Internet ads, identify every URL, date, and number of

hits or visits; for all other materials, provide sufficient information to permit a determination of how many items were disseminated, and when, where, and to whom such items were disseminated.

B. For each product or service identified in response to 3.A. and each item of personal data identified in response to 4.A., identify any keywords, terms, phrases, or other criteria that the Company has used to effect the placement or delivery of any advertisement or sponsored link in connection with any online advertising network or advertisement delivery or contextual marketing software or system, including but not limited to the placement or delivery of any advertisement or sponsored link in search results generated by any Internet search engine.

9. **Complaints/Inquiries:**

A. State the number of complaints or disputes related to data collection, use, aggregation, or display the Company has received on an annual basis. Describe in detail the Company's process for recording consumer complaints or disputes related to data collection, use, aggregation, or display, including, but not limited to, any categorization of the complaints or disputes and the Company's response to the complaints or disputes. Provide copies of all documentation of complaints or disputes and the Company's response.

B. State whether the Company has been the subject of any government or regulatory inquiry or private action. Identify each such inquiry or action and describe the nature of the inquiry or action, the practices investigated or at issue, the violations of law investigated or alleged, and the status or outcome of the inquiry or action. For government or regulatory inquiries, identify the agency or entity conducting the inquiry and the name and contact information for the Company's contact person at such agency or entity. For each private action, identify the court in which the action was filed, the date it was filed, and its docket number.

The Special Report responses called for in this Order are to be filed no later than **February 1, 2013**.

All responses for all Specifications must be provided in narrative form in two (2) printed copies and in electronic form (by CD or as email attachments), formatted as Word or WordPerfect documents. In addition, electronic responses to Specifications 3-6 must also be provided on the Excel spreadsheets included as Attachments B, C, and D to this Order.[1] Documentary responses

[1]An electronic version of the Excel spreadsheets for Attachments B, C, and D are provided on the included CD. The company must use Attachments B, C, and D to report

must be formatted as Adobe Acrobat documents. All responses must be labeled to indicate the Specification to which the information or data responds. All files contained in electronic submissions must have a file name that includes the company name, Specification numbers included in the file, and date of the submission, in the following format: **[COMPANYNAME]_Spec._[SPEC. #'S]_[MM-DD-YY]**.

Penalties may be imposed under applicable provisions of federal law for failure to file Special Reports or for filing false reports.

By the Commission.

_____
Jon Leibowitz
Chairman

SEAL
Date of Order: December 14, 2012

The Special Report required by this Order, or any inquiry concerning it, should be addressed to the attention of:

Peder Magee
Federal Trade Commission
Division of Privacy and Identity Protection
601 New Jersey Avenue, N.W., NJ-8100
Washington, D.C. 20580
(202) 326-3538 phone
(202) 326-3062 facsimile
pmagee@ftc.gov

or

Tiffany George
Federal Trade Commission
Division of Privacy and Identity Protection
601 New Jersey Avenue, N.W., NJ-8100
Washington, D.C. 20580
(202) 326-3040 phone
(202) 326-3062 facsimile
tgeorge@ftc.gov

---

activities and must not modify, delete, or add to the columns on the spreadsheet. The company must submit the spreadsheets in Excel in a format that is readable and writable and must not include footnotes or endnotes on the spreadsheet.

Attachment A

DEFINITIONS & ADDITIONAL INSTRUCTIONS

A. "**Advertisement**" or "**advertising**" or "**ad**" or **"promotional material**" shall mean any written or verbal statement, illustration, or depiction, whether in English or any other language, that is designed to effect a sale or create interest in the purchasing of goods or services, whether it appears on or in a label, package, package insert, radio, television, cable television, brochure, newspaper, magazine, pamphlet, leaflet, circular, mailer, book insert, free standing insert, letter, catalogue, poster, chart, billboard, public transit card, point of purchase display, film, slide, audio program transmitted over a telephone system, telemarketing script, onhold script, upsell script, training materials provided to telemarketing firms, program-length commercial ("infomercial"), the Internet, email, or any other medium.

B. **"Personal data**" shall mean information from or about consumers, including, but not limited to: (1) first and last name; (2) home or other physical address, including street name and name of city or town; (3) email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) telephone number; (5) date of birth; (6) gender, racial, ethnic, or religious information; (7) government-issued identification number, such as a driver's license, military identification, passport, or Social Security number, or other personal identification number; (8) financial information, including but not limited to: investment account information; income tax information; insurance policy information; checking account information; and credit, debit, or check-cashing card information, including card number, expiration date, security number (such as card verification value), information stored on the magnetic stripe of the card, and personal identification number; (9) employment information, including, but not limited to, income, employment, retirement, disability, and medical records; or (10) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

C. **"Product or service"** shall not include those products or services that are "consumer reports" as set forth in the Fair Credit Reporting Act, 15 U.S.C. § 1681a(d).

D. **Meet and Confer:** You are encouraged to contact **Peder Magee** at **(202) 326-3538** or **Tiffany George** at **(202) 326-3040** as soon as possible to schedule a meeting (telephonic or in person) in order to confer regarding your response.

E. **Applicable Time Period:** Unless otherwise directed in the specifications, the applicable time period for the request shall be from **January 1, 2010 until the date of full and complete compliance with this Order**.

F. **Document Production:** Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS.

G. **Production of Copies:** Copies of marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

H. **Sensitive Personally Identifiable Information:** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact us before sending those materials to discuss ways to protect such information during production.

For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

APPENDIX B: Illustrative List of Data Elements and Segments

Illustrative List of Data Elements and Segments

Identifying Data

- Name
- Previously Used Names
- Address
- Address History
- Longitude and Latitude
- Phone Numbers
- Email Address

Sensitive Identifying Data

- Social Security Number
- Driver's License Number
- Birth Date
- Birth Dates of Each Child in Household
- Birth Date of Family Members in Household

Demographic Data

- Age
- Height
- Weight
- Gender
- Race & Ethnicity
- Country of Origin
- Religion (by Surname at the Household Level)
- Language
- Marital Status
- Presence of Elderly Parent
- Presence of Children in Household
- Education Level
- Occupation
- Family Ties
- Demographic Characteristics of Family Members in Household
- Number of Surnames in Household
- Veteran in Household
- Grandparent in House
- Spanish Speaker
- Foreign Language Household (e.g., Russian, Hindi, Tagalog, Cantonese)
- Households with a Householder who is Hispanic Origin or Latino
- Employed - White Collar Occupation
- Employed - Blue Collar Occupation
- Work at Home Flag
- Length of Residence
- Household Size
- Congressional District
- Single Parent with Children
- Ethnic and Religious Affiliations

Court and Public Record Data

- Bankruptcies
- Criminal Offenses and Convictions
- Judgments
- Liens
- Marriage Licenses
- State Licenses and Registrations (e.g., Hunting, Fishing, Professional)
- Voting Registration and Party Identification

Social Media and Technology Data

- Electronics Purchases
- Friend Connections
- Internet Connection Type

- Internet Provider
- Level of Usage
- Heavy Facebook User
- Heavy Twitter User
- Twitter User with 250+ Friends
- Is a Member of over 5 Social Networks
- Online Influence
- Operating System
- Software Purchases
- Type of Media Posted
- Uploaded Pictures
- Use of Long Distance Calling Services
- Presence of Computer Owner
- Use of Mobile Devices
- Social Media and Internet Accounts including: Digg, Facebook, Flickr, Flixster, Friendster, hi5, Hotmail, LinkedIn, Live Journal, MySpace, Twitter, Amazon, Bebo, CafeMom, DailyMotion, Match, myYearbook, NBA.com, Pandora, Photobucket, WordPress, and Yahoo

Home and Neighborhood Data

- Census Tract Data
- Address Coded as Public/Government Housing
- Dwelling Type
- Heating and Cooling
- Home Equity
- Home Loan Amount and Interest Rate
- Home Size
- Lender Type
- Length of Residence
- Listing Price
- Market Value
- Move Date
- Neighborhood Criminal, Demographic, and Business Data
- Number of Baths
- Number of Rooms
- Number of Units
- Presence of Fireplace
- Presence of Garage
- Presence of Home Pool
- Rent Price
- Type of Owner
- Type of Roof
- Year Built

General Interest Data

- Apparel Preferences
- Attendance at Sporting Events
- Charitable Giving
- Gambling - Casinos
- Gambling - State Lotteries
- Thrifty Elders
- Life Events (e.g., Retirement, Newlywed, Expectant Parent)
- Magazine and Catalog Subscriptions
- Media Channels Used
- Participation in Outdoor Activities (e.g., Golf, Motorcycling, Skiing, Camping)
- Participation in Sweepstakes or Contests
- Pets
- Dog Owner
- Political Leanings
- Assimilation Code
- Preferred Celebrities
- Preferred Movie Genres
- Preferred Music Genres
- Reading and Listening Preferences
- Donor (e.g., Religious, Political, Health Causes)
- Financial Newsletter Subscriber
- Upscale Retail Card Holder
- Affluent Baby Boomer
- Working-Class Moms
- Working Woman
- African-American Professional
- Membership Clubs - Self-Help

- Membership Clubs - Wines
- Exercise - Sporty Living
- Winter Activity Enthusiast
- Participant - Motorcycling
- Outdoor/Hunting & Shooting
- Biker/Hell's Angels
- Santa Fe/Native American Lifestyle
- New Age/Organic Lifestyle
- Is a Member of over 5 Shopping Sites
- Media Channel Usage - Daytime TV
- Bible Lifestyle
- Leans Left
- Political Conservative
- Political Liberal
- Activism & Social Issues

Financial Data

- Ability to Afford Products
- Credit Card User
- Presence of Gold or Platinum Card
- Credit Worthiness
- Recent Mortgage Borrower
- Pennywise Mortgagee
- Financially Challenged
- Owns Stocks or Bonds
- Investment Interests
- Discretionary Income Level
- Credit Active
- Credit Relationship with Financial or Loan Company
- Credit Relationship with Low-End Standalone Department Store
- Number of Investment Properties Owned
- Estimated Income
- Life Insurance
- Loans
- Net Worth Indicator
- Underbanked Indicator
- Tax Return Transcripts
- Type of Credit Cards

Vehicle Data

- Brand Preferences
- Insurance Renewal
- Make & Model
- Vehicles Owned
- Vehicle Identification Numbers
- Vehicle Value Index
- Propensity to Purchase a New or Used Vehicle
- Propensity to Purchase a Particular Vehicle Type (e.g., SUV, Coupe, Sedan)
- Motor Cycle Owner (e.g., Harley, Off-Road Trail Bike)
- Motor Cycle Purchased 0-6 Months Ago
- Boat Owner
- Purchase Date
- Purchase Information
- Intend to Purchase - Vehicle

Travel Data

- Read Books or Magazines About Travel
- Travel Purchase - Highest Price Paid
- Date of Last Travel Purchase
- Air Services - Frequent Flyer
- Vacation Property
- Vacation Type (e.g., Casino, Time Share, Cruises, RV)
- Cruises Booked
- Preferred Vacation Destination
- Preferred Airline

Purchase Behavior Data

- Amount Spent on Goods
- Buying Activity
- Method of Payment
- Number of Orders
- Buying Channel Preference (e.g., Internet, Mail, Phone)

- Types of Purchases
- Military Memorabilia/Weaponry
- Shooting Games
- Guns and Ammunition
- Christian Religious Products
- Jewish Holidays/Judaica Gifts
- Kwanzaa/African-Americana Gifts
- Type of Entertainment Purchased
- Type of Food Purchased
- Average Days Between Orders
- Last Online Order Date
- Last Offline Order Date
- Online Orders $500-$999.99 Range
- Offline Orders $1000+ Range
- Number of Orders - Low-Scale Catalogs
- Number of Orders - High-Scale Catalogs
- Retail Purchases - Most Frequent Category
- Mail Order Responder - Insurance
- Mailability Score
- Dollars - Apparel - Women's Plus Sizes
- Dollars - Apparel - Men's Big & Tall
- Books - Mind & Body/Self-Help
- Internet Shopper
- Novelty Elvis

Health Data

- Ailment and Prescription Online Search Propensity
- Propensity to Order Prescriptions by Mail
- Smoker in Household
- Tobacco Usage
- Over the Counter Drug Purchases
- Geriatric Supplies
- Use of Corrective Lenses or Contacts
- Allergy Sufferer
- Have Individual Health Insurance Plan
- Buy Disability Insurance
- Buy Supplemental to Medicare/Medicaid Individual Insurance
- Brand Name Medicine Preference
- Magazines - Health
- Weight Loss & Supplements
- Purchase History or Reported Interest in Health Topics including: Allergies, Arthritis, Medicine Preferences, Cholesterol, Diabetes, Dieting, Body Shaping, Alternative Medicine, Beauty/Physical Enhancement, Disabilities, Homeopathic Remedies, Organic Focus, Orthopedics, and Senior Needs

APPENDIX C: Concurring Statement of Commissioner Julie Brill

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

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.

about the sources of data brokers' information, help give 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 their subsequent use of the information, often fall outside of the context in which consumers provide the information, prominent

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 48-50 (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.

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 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

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.

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.

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 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 informa-

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.

18 *See, e.g.*, Data Broker Report, *supra* note 1, at 52-53.

19 *See id.* at 37, 52-53.

tion 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 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

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.

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.

Federal Trade Commission
May 2014