

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

on

What Information Do Data Brokers Have On Consumers, And How Do They Use It

Before the

COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

December 18, 2013

I. Introduction

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, I am Jessica Rich, Director of the Bureau of Consumer Protection of the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s testimony on data brokers.

Data brokers collect and aggregate consumers’ personal information from a wide range of sources and resell it for an array of purposes, such as marketing, verifying an individual’s identity, and preventing financial fraud. Because data brokers generally never interact directly with consumers, consumers are typically unaware of their existence, much less the variety of ways they collect, analyze, and sell consumer data.

This Committee, by investigating the privacy practices of data brokers, has helped call attention to the lack of transparency surrounding data broker privacy practices. We look forward to reviewing the Committee’s report on its examination of the data broker industry. We commend Chairman Rockefeller’s leadership on this issue and stand ready to work with this Committee and Congress on ways to improve the transparency of data broker practices. As the Committee is aware, the Commission is developing its own report on the data broker industry (discussed further below), which the Commission expects to release in the coming months.

This testimony begins by describing the Commission’s longstanding work in this area. It then lays out our strategy for addressing the privacy practices of the data broker industry through enforcement, research and reports, and business and consumer education.

¹ This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or any Commissioner.

II. Background on FTC Initiatives Concerning Data Broker Privacy Practices

Concerns about the privacy practices of companies that buy and sell consumer data are not new. Indeed, in 1970, the existence of companies selling consumer data with little transparency for credit and other eligibility determinations led Congress to enact the Fair Credit Reporting Act (FCRA)², which it gave the Commission authority to enforce.

In the late 1990s, the Commission began to examine the privacy practices of data brokers that fall outside the FCRA.³ Notably, 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 Reference Services Group (IRSG).⁴ The Commission subsequently issued a report on the workshop and the IRSG. The report commended the progress made by the industry’s self-regulatory programs, but one of the report’s conclusions was that the industry’s efforts did not adequately address the lack of transparency of data broker practices. Although industry ultimately terminated the IRSG, a series of public breaches – including one involving ChoicePoint – led to renewed scrutiny of the practices of data brokers.⁵

² 15 U.S.C. § 1681 et seq.

³ See, e.g., FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), available at <http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml>; Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (Mar. 10, 2005), available at <http://www.ftc.gov/public-statements/2005/03/prepared-statement-federal-trade-commission-identity-theft-recent>; see also FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), available at <http://www.ftc.gov/news-events/events-calendar/2003/06/information-flows-costs-and-benefits-related-collection-and-use>.

⁴ See FTC, *Individual Reference Services, A Report to Congress* (1997), available at <http://www.ftc.gov/reports/individual-reference-services-report-congress>.

⁵ This scrutiny included an FTC investigation that resulted in the FTC’s largest FCRA civil penalty to date. See *United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198 (N.D. Ga. Feb. 15, 2006) (stipulated final order imposing \$10 million fine and \$5 million in consumer redress), available at <http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf>.

Most recently, in its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Consumers* (Privacy Report),⁶ the Commission specifically addressed the privacy practices 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.⁷ The report noted that, while the FCRA gives consumers a variety of rights with regard to companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories operate without much transparency.

Building on the agency's prior work, the Commission's Privacy Report made recommendations to improve the transparency of the practices of data brokers and to give consumers greater control over how their information is used. Among other things, the Report proposed that data brokers provide consumers with reasonable access to the data they maintain. The Report also noted that the Commission had long supported legislation that would give access rights to consumers for information held by data brokers.⁸ The Report stated that the Commission continues to support legislation in this area to improve the transparency of industry practices.⁹

III. The Commission's Ongoing Initiatives Regarding Data Brokers

The Commission's ongoing initiatives to address the privacy practices of the data broker

⁶ FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>. Commissioner Wright's term as Commissioner began in January 2013 and he was not at the Commission when the Privacy Report was issued. While he may not necessarily endorse all the views in that Report, he agrees with the substance of this testimony.

⁷ *Id.* at 65.

⁸ *Id.* at 69.

⁹ *Id.*

industry build on this body of prior work. The Commission is pursuing a three-pronged strategy to ensure consumer interests are protected in the data broker context. First, the Commission takes aggressive enforcement action to ensure that data brokers comply with the FCRA where it applies. Second, as data broker business models expand beyond traditional credit reporting, the FTC continues to conduct research and issue reports examining the practices of the data broker industry. Third, the Commission educates businesses about their legal responsibilities, especially small data brokers that may be unaware of their legal obligations, and consumers regarding how their data is disseminated. These three initiatives are discussed below.

A. Enforcement

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. FCRA enforcement is a vital priority for the agency, particularly as companies that are not traditional credit reporting agencies venture into territory covered by the FCRA.¹⁰

For example, last year the Commission entered into a consent decree with online data broker Spokeo to resolve allegations that the company violated the FCRA.¹¹ As set forth in the Commission's complaint, Spokeo assembled personal information from hundreds of online and offline data sources, including social networks, and merged that data to create detailed personal profiles, including name, address, age range, hobbies, ethnicity, and religion. Spokeo marketed these profiles for use by human resources departments in hiring decisions. The FTC alleged that

¹⁰ The FCRA provides basic consumer protections when consumer reporting data is used to make eligibility determinations for credit, insurance, employment and similar purposes.

¹¹ *United States v. Spokeo, Inc.*, No. CV12-05001 (C.D. Cal. June 12, 2012), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2012/06/spokeo-inc-united-states-america-federal-trade>; see also Press Release, FTC, *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA* (June 12, 2012), available at <http://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

Spokeo, which marketed profiles for employment purposes, was a consumer reporting agency subject to the FCRA. The Commission charged Spokeo with violating the FCRA by, among other things, failing to (1) take reasonable steps to ensure the accuracy of information; and (2) tell its clients about their obligations under the FCRA, including the requirement to send adverse action notices to people denied employment on the basis of information obtained from Spokeo. The order contained strong injunctive relief and an \$800,000 civil penalty.

The Commission also recently took action against a mobile application developer that compiled and sold criminal record reports without complying with the FCRA.¹² The app developer, Filiquarian, claimed that consumers could use its mobile apps to access hundreds of thousands of criminal records and conduct searches on potential employees. The FTC charged that Filiquarian failed to take reasonable steps to ensure that the information it sold was accurate and would be used solely for permissible purposes, as required by the FCRA. In addition, Filiquarian failed to inform users of its reports of their obligations under the FCRA, including the requirement to notify consumers if an adverse action was taken against them based on a report. In both the Spokeo and Filiquarian cases, the companies' terms of service included disclaimers stating that the information they provided should not be used for FCRA purposes. Despite these disclaimers, the companies specifically advertised that their reports could be used for employment purposes.

Most recently, the Commission entered into a consent decree with Certegy Check

¹² Decision and Order, *Filiquarian Publishing, LLC*, FTC File No. 112-3195 (May 1, 2013), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/05/filiquarian-publishing-llc-choice-level-llc-and>; see also Press Release, FTC, *FTC Approves Final Order Settling Charges Against Marketers of Criminal Background Screening Reports* (May 1, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/05/ftc-approves-final-order-settling-charges-against-marketers>.

Services, one of the nation's largest check authorization service companies.¹³ Certegy compiles consumers' personal information and uses it to help retail merchants determine whether to accept consumers' checks. The Commission's complaint alleged that, among other things, when a merchant denied a consumer's check, and the consumer contacted Certegy to dispute the denial, the company failed to follow proper dispute procedures, as required by the FCRA. As a result, Certegy's denials may have been in error, and consumers may not have been able to pay for essential goods and services. Certegy agreed to pay \$3.5 million, the agency's second largest FCRA fine, to resolve the Commission's allegations.

B. Research and Reports

The Commission is devoting significant resources to research and reports addressing the privacy practices of data brokers. As described above, the Commission's Privacy Report discussed the data broker industry specifically and recommended steps data brokers should take to improve the transparency of data broker practices and give consumers greater control over their information.¹⁴

To undertake a more detailed examination of the data broker industry, the Commission issued orders requiring nine data brokers to provide the agency with information regarding how they collect and use consumer data. The orders, issued pursuant to the Commission's authority under Section 6(b) of the FTC Act, mandated production of detailed information regarding company practices, including the nature and sources of consumer data the companies collect, how they use, maintain, and disseminate the information, and the extent to which the data

¹³ *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/08/certegy-check-services-inc>; see also Press Release, FTC, *Certegy Check Services to Pay \$3.5 Million for Alleged Violations of the Fair Credit Reporting Act and Furnisher Rule* (Aug. 15, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/08/certegy-check-services-pay-35-million-alleged-violations-fair>.

¹⁴ *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 6, at 68-70.

brokers allow consumers to access and correct their information or to opt out of having their personal information sold. These orders were directed to companies providing three basic non-FCRA services – marketing services, risk mitigation services, including identity verification and fraud detection, and people search or look-up services. The Commission is expects to release a report on this examination of the data broker industry in the coming months.

We also continue to examine emerging practices in the data broker industry. Just this month, we announced a series of seminars for early 2014 that will address a number of consumer privacy issues, including alternative scoring products offered by data brokers. Many data brokers offer companies scores to predict trends and the behavior of their customers. Companies are using predictive scores for a variety of purposes, ranging from identity verification and fraud prevention to marketing and advertising. Consumers are largely unaware of these scores and have little to no access to the underlying data from which they are derived. The program will explore a number of issues, including what scores are currently available, how companies are using them, how accurate the scores and underlying data are, privacy concerns surrounding the use of predictive scoring, how consumers can benefit from use of these scores, and what sort of consumer protections should exist for them.¹⁵

C. Education

In addition to its enforcement and policy work on data broker issues, the agency also focuses on educating businesses and consumers about these issues. An important method for educating businesses is to publicize Commission complaints and orders and issue public letters warning companies of legal requirements and/or potential violations. In this vein, the

¹⁵ Press Release, FTC, *Spring Privacy Series: Alternative Scoring Products* (Mar. 19, 2014), available at <http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products>.

Commission sent staff warning letters to a number of data brokers that provided tenant-screening services, and to marketers of six mobile apps that provide employment background screening services.¹⁶ The FTC warned the companies and app developers that, if they have reason to believe the reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA.¹⁷

More recently, Commission staff conducted an undercover effort to determine if data brokers that disclaimed FCRA liability were willing to sell information for credit, insurance, employment, or housing decisions. As a result of this “test shopping” operation, Commission staff found ten data brokers who appeared to offer data for these purposes. Commission staff then sent warning letters to these companies, advising them that their practices could violate the FCRA.¹⁸

The FTC also hosts a Business Center blog,¹⁹ which frequently includes consumer privacy and data security topics; currently, approximately 3,500 attorneys and business executives subscribe to these email blog updates. The Business Center blog consistently features the Commission’s enforcement actions and warning letters.

Finally, the FTC has developed materials designed to educate consumers about the ways in which their data may be disseminated to companies with which they do not interact. For

¹⁶ Press Release, FTC, *FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act* (Apr. 3, 2013), available at <http://www.ftc.gov/opa/2013/04/tenant.shtm>; Press Release, FTC, *FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), available at <http://www.ftc.gov/opa/2012/02/mobileapps.shtm>.

¹⁷ The Commission made no determination as to whether the companies were violating the FCRA, but encouraged them to review their apps and their policies and procedures to ensure they comply with the Act.

¹⁸ Press Release, FTC, *FTC Warns Data Broker Operations of Possible Privacy Violations* (May 7, 2013), available at <http://www.ftc.gov/opa/2013/05/databroker.shtm>.

¹⁹ See generally <http://business.ftc.gov/blog>.

example, the FTC produced a video called *Sharing Information: A Day in Your Life*, that describes how everyday activities by consumers – shopping in retail stores with loyalty cards, buying good online, and using social networking services – can lead to wide dissemination of personal information.²⁰

IV. Conclusion

These enforcement, policy, and education efforts demonstrate the Commission's continued commitment to understanding and addressing consumer privacy issues posed by the data broker industry. We appreciate the leadership of Chairman Rockefeller and this Committee on these issues and look forward to continuing to work with Congress, industry, and other critical stakeholders on these issues in the future.

²⁰ FTC, *Sharing Information: A Day in Your Life*, available at <http://www.consumer.ftc.gov/media/video-0022-sharing-information-day-your-life>.