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 at 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 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.[5] 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.[6]

---

[2] 15 U.S.C. § 1681 et seq.

[3] See, e.g.

Most recently, in its 2012 report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Consumers (Privacy Report),[5] 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

III. The Commission's Ongoing Initiatives Regarding Data Brokers

The Commission's ongoing initiatives to address the privacy practices of the data broker industry build on this body of prior work. The Commission is pursuing a three-pronged strategy

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 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

3.445 from Spokeo.

disclaimers, the companies specifically advised that their reports could be used for employment purposes.

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

[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-

under Section 6(b) of the FTC Act, mandated production of detailed information regarding company practices, including the nature and scope of consumer data the companies collect, how they use, maintain, and disseminate the information, and the extent to which the data 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

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 potential violations. In this vein, the 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 mu

The FTC also hosts a Business Center blog,[19] which frequently includes consumer privacy and data security