

Reproduced with permission from Social Media Law Reporter, 01 SMLR 14, 07/31/2012. Copyright © 2012 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Advertising & Marketing

The Federal Trade Commission recently brought its first case concerning the sale of internet and social media data in the employment screening context. This case and other actions by the FTC discussed in this article serve as a reminder that companies that collect and market data to third parties must be careful about making representations that could inadvertently trigger laws governing specific regulated industries, the authors write. Moreover, firms must also be aware of and monitor the activities of the new cop on the beat overseeing consumer financial products and services, the Consumer Financial Protection Bureau.

Blurring Lines and Increased Regulatory Risks for Data Brokers

BY MARC S. ROTH AND CHARLES WASHBURN

The data broker industry is very much on the radar of regulators. In various forms, the Federal Trade Commission (FTC) has made it clear that entities that collect and aggregate consumer information on a large scale from various sources are one of its highest priorities. This position was made very clear recently when the agency brought an action against an online company that sells consumer data collected through various social media sites. As the company marketed its list for specific purposes, such as employment screening, the FTC claimed that the company was acting as a credit reporting bureau, but failed to comply with applicable federal laws. This case and other actions by the

FTC discussed in this article serve as a reminder that companies that collect and market data to third parties must be careful about making representations that could inadvertently trigger laws governing specific regulated industries. Moreover, in addition to following FTC actions in this area, firms must also be aware of and monitor the activities of the new cop on the beat overseeing consumer financial products and services, the Consumer Financial Protection Bureau (CFPB).

The FTC Looks at Data Brokers

In its privacy report released earlier this year titled *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC first enunciated its concerns about data brokers.¹ The report recommended that legislation be introduced to regulate the data brokerage industry,

Marc S. Roth and Charles Washburn are partners at Manatt, Phelps & Phillips LLP. Roth, who practices in Manatt's New York City office, is a member of the firm's nationally recognized Advertising, Marketing & Media Division, where he specializes in privacy and data security matters and regulatory defense. Washburn practices in Manatt's Los Angeles office, where he assists clients in complying with federal and state consumer credit and other financial laws, including compliance with FCRA. Stacey Mayer, an associate in the New York office, assisted in the preparation of this article.

noting the risks associated with this industry given that data brokers collect massive amounts of information about consumers from various sources with little or no transparency and accountability, and the absence of specific laws in this area. It is estimated that each of the three largest consumer reporting agencies in the country maintain files on about 200 million Americans, culled from about 10,000 information providers, that about 3 billion credit reports are issued each year, and that 36 billion updates are made to consumer credit files annually.² In addition to calling for legislation in this area, the FTC also urged companies in this industry to become more transparent to consumers, by allowing access to and the ability for consumers to correct inaccurate information in the files they maintain.

Commissioner Julie Brill reiterated the agency's concern with data brokers at a privacy conference this past spring, noting that this industry is one of the FTC's top three priorities.³ Brill also commented in a recent *New York Times* article about the data broker Acxiom, that she "would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used."⁴ Further, Brill would like to have these companies disclose to consumers "how information has been analyzed to place the consumer into certain categories for marketing purposes," noting that "giving consumers this kind of granularity will greatly increase consumer trust in the information flow processes and will lead to more accurate marketing."⁵

Commission Chairman Jon Leibowitz has echoed Commissioner Brill's sentiments, noting that consumers should have the right to see and correct personal de-

tails about them collected and sold by data aggregators.⁶

Not long thereafter, the FTC backed up its words by announcing that it had settled charges against a data broker for violating the Fair Credit Reporting Act (FCRA). Specifically, the FTC alleged that data broker Spokeo collected information about consumers from hundreds of online and offline sources, including social media networks, data brokers, and other sources, and used that data to create detailed profiles of consumers (including a person's name, age, hobbies, ethnicity, religion, use of social media, and photos), which it marketed to human resources professionals, recruiters, and others as an employment screening tool.⁷ This was the agency's first case concerning the sale of internet and social media data in the employment screening context.⁸

Based on these activities, the FTC alleged that Spokeo operated as a consumer reporting agency but failed to take the necessary steps that FCRA mandates to ensure that the information they provide will be used for legitimate business purposes, to maintain the integrity of the data, and to provide notice to consumers of their ability to review and correct inaccurate information about them, thereby violating the FCRA.⁹

Moreover, despite Spokeo's changing its website Terms of Service in 2010 to state that it was not a consumer reporting agency and that clients could not use the company's website or information for FCRA purposes, according to the FTC the company failed to revoke access to companies using data for that purpose, such as subscribers who signed up via the spokeo.com/HR page or who bought subscriptions in response to marketing to human resources professionals.

The Spokeo case followed warning letters sent by the FTC to three mobile app marketers earlier this year, which suggested that their background screening apps may be violating the FCRA.¹⁰ Those letters warned that if the app developers have reason to believe that the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA.

Spokeo agreed to settle the FTC's charges by entering into a consent decree that includes payment of an \$800,000 civil penalty, various injunctive provisions, and a ban on further violations of the FCRA.¹¹ Although the Spokeo settlement applies only to Spokeo, the case offers insight for any company that collects and markets consumer data to third parties. This guidance is particularly interesting given that Spokeo, like the three app developers, does not appear to fall within the purview of the FCRA as a consumer reporting agency.

¹ *FTC Report: Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

² Evan Weinberger, *CFPB Set to Replace Patchwork Credit Reporting Co. Regime*, *LAW360* (July 16, 2012); Stuart Pratt, Comments of CDIA to National Telecommunications and Information Administration, "Information Privacy and Innovation in the Internet Economy," at 2 (June 13, 2010), available at <http://ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/Consumer%20Data%20Industry%20Association%20Comments.pdf>; Stuart Pratt, President, CDIA, Statement Before House Committee on Financial Institutions and Consumer Credit, "Keeping Score on Credit Scores: An Overview of Credit Scores, Credit Reports, and Their Impact on Consumers," at 7 (March 24, 2010), available at http://www.house.gov/apps/list/hearing/financialsvcs_dem/pratt_testimony.pdf; see also *FTC Report to Congress under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 8-9 (2004); Stuart Pratt, Statement Before House Committee on Financial Services, "Credit Reports: Consumer's Ability to Dispute and Change Inaccurate Information," at 23 (June 19, 2007), available at <http://archives.financialservices.house.gov/hearing110/ospratt061907.pdf>.

³ Allison Grande, *Mobile, Data Brokers Among FTC's Top Priorities, Brill Says*, *LAW360* (June 19, 2012), <http://www.law360.com/articles/351628/mobile-data-brokers-among-ftc-s-top-priorities-brill-says>.

⁴ Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, *THE NEW YORK TIMES* (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=1&pagewanted=all.

⁵ Natasha Singer, *Consumer Data, but Not for Consumers*, *THE NEW YORK TIMES* (July 21, 2012), <http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all>.

⁶ *Id.*

⁷ *FTC v. Spokeo Inc.*, No. CV12-05001, FTC File No. 1023163, Complaint, available at <http://ftc.gov/os/caselist/1023163/120612spokeocmpt.pdf>.

⁸ *FTC v. Spokeo Inc.*, No. CV12-05001, FTC File No. 1023163, available at <http://ftc.gov/os/caselist/1023163/index.shtm>.

⁹ Press Release, Federal Trade Commission, *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>.

¹⁰ 15 U.S.C. §§ 1681 *et seq.*

¹¹ *Spokeo Inc.*, No. CV12-05001, Consent Decree, available at <http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf>.

A Review of the Fair Credit Reporting Act

Prior to the adoption of the FCRA, the business of collecting information about consumers and selling reports based on that information generally was unregulated. This caused problems for both consumers and the reporting industry. For example, there was no specific requirement that information in the sellers' files be accurate. Inaccurate information can lead to a consumer being unfairly turned down for a loan, a job, or an apartment, among other things. Inaccurate information also makes reports less useful to users. There was no obligation to tell the consumer that a report had been used in a transaction, so the consumer would be unaware that he or she might have been turned down based on inaccurate information. There also was no limit on the purposes for which someone could obtain a report on a consumer, raising significant privacy concerns. From an industry perspective, inconsistent state laws presented challenges for nationwide sellers of reports.

To address these problems, Congress passed the FCRA in 1970. The FCRA has been amended several times since, with major changes adopted in 1996 and 2003,¹² and most recently in 2010 pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).¹³

The FCRA addressed the problems that existed before it was adopted, requiring a "consumer reporting agency" (CRA) to ensure the accuracy of information in its files, and allowing consumers the ability to dispute the accuracy of the information. Additionally, the FCRA requires a "furnisher of information" to submit accurate information and provides that such furnishers of information can be brought into disputes regarding accuracy. Finally, the FCRA requires a "user" of a "consumer report" to provide a notice to the consumer when the user takes "adverse action" based on the report. A consumer report can be obtained by a user only for certain "permissible purposes," protecting consumers' privacy. The FCRA also generally preempts state consumer reporting laws, with a limited number of specific exceptions, facilitating nationwide consumer reporting operations.

Interestingly, in the *New York Times* article referenced above, Commissioner Brill is cited as comparing the reluctance of the data broker industry to make consumer records available today to the pre-FCRA era when CRAs argued that it would be too expensive and time-consuming for them to show individuals the same reports that creditors could see.¹⁴ Brill has stated that the data broker industry could do "the exact same thing" as the credit reporting industry.¹⁵

¹² The 2003 changes were made pursuant to the Fair and Accurate Credit Transactions Act of 2003, which is also called the "FACT Act" or "FACTA." See FACTA, Pub. L. 108-159, H.R. 2622, 108th Cong. (Dec. 4, 2003), available at <http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/html/PLAW-108publ159.htm>.

¹³ Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, H.R. 4173, 111th Cong. (July 21, 2011) (12 U.S.C. §§ 5301 *et seq.*), available at <http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/content-detail.html>.

¹⁴ See n.5, *supra*.

¹⁵ *Id.*

What Is a "Consumer Reporting Agency" and What Is a "Consumer Report"?

The FCRA generally defines a CRA as a person who, for compensation, regularly assembles or evaluates information about consumers for the purpose of furnishing consumer reports to third parties.¹⁶ A consumer report, in turn, is a communication of information by a CRA bearing on one of seven characteristics (i.e., credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living) and used or expected to be used or collected for a "permissible purpose" under the FCRA, including for use in decisioning credit, employment, rental of an apartment, or a transaction initiated by a consumer.¹⁷

There are a number of things to note from these definitions. First, they are circular: a CRA is a person who furnishes consumer reports, and a consumer report is a communication of information by a CRA.

Second, although CRAs are commonly referred to as "credit bureaus" and consumer reports are usually called "credit reports" or "credit scores," a report can qualify as a consumer report if it contains noncredit information that bears on one or more of the seven characteristics, and a CRA can provide reports used in non-credit contexts such as renting an apartment or applying for a job. Indeed, this was the case with Spokeo and the mobile app developers to whom the FTC sent warning letters, as these companies are not traditional CRAs, in that they do not obtain and aggregate consumer credit history data, as do the three largest and most well-known bureaus, TransUnion, Equifax, and Experian.

Third, and although perhaps counterintuitive, a person generating reports on consumers that bear on one or more of the seven characteristics, but that are not used or expected to be used or collected for FCRA-permissible purposes, is not a CRA and therefore is outside of the scope of the FCRA. This would include, for example, an information services company that generates reports that are used solely for target marketing purposes.

Jurisdiction Over Credit Reporting Agencies

The stakes for data brokers are increasing, particularly with respect to potential regulatory enforcement. For many years, the FCRA was interpreted and enforced by the FTC with respect to non-banks, and the *Spokeo* case evidences the agency's expansive interpretation of this law. However, a new federal agency now shares jurisdiction over the FCRA with the FTC. The CFPB, which was created by Dodd-Frank, "opened for business" on July 21, 2011, when the authority to interpret a number of federal consumer protection laws, including most provisions of the FCRA, was transferred to the CFPB along with enforcement authority with respect to the transferred laws. Because Dodd-Frank did not entirely remove the FTC's enforcement authority under the FCRA, the FTC and CFPB have entered into a Memorandum of Understanding, as required by Dodd-Frank, pursuant to which the FTC and CFPB generally

¹⁶ 15 U.S.C. § 1681A(f).

¹⁷ 15 U.S.C. § 1681A(d).

are required to coordinate their enforcement activities with respect to non-banks.¹⁸

Dodd-Frank granted the CFPB authority to supervise certain “nonbank “covered persons” for compliance with federal consumer financial laws and other purposes, including nonbank “larger participants” in certain “markets” for consumer financial products.¹⁹ A final rule published in the Federal Register on July 20, which takes effect on Sept. 30, establishes the “consumer reporting” market as the initial market identified by the CFPB, and provides that participants in this market with annual receipts from consumer reporting of more than \$7 million are deemed to be “larger participants” in that market.²⁰ Such larger participants in the consumer reporting market will be subject to CFPB supervision, which supervision entails regular CFPB examinations and the filing of periodic reports with CFPB. Such examinations will review how credit reporting companies will compile their reports and ensure their accuracy, and otherwise will examine the company for compliance with all of the requirements of FCRA. CRAs have not previously been subject to such intensive federal examinations.

Only data brokers with more than \$7 million in annual receipts resulting from relevant consumer reporting activities would be subject to CFPB supervision. This clearly includes the “Big Three” credit bureaus,

¹⁸ Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission (Jan. 20, 2012), available at <http://ftc.gov/os/2012/01/120123ftc-cfpb-mou.pdf>.

¹⁹ 12 U.S.C. § 5514.

²⁰ Defining Larger Participants of the Consumer Reporting Market, 77 Fed. Reg. 42,874 (July 20, 2012) (to be codified at 12 C.F.R. pt. 1090).

and CFPB estimates that approximately 30 CRAs will meet this test. However, it is important to keep in mind that there is no minimum annual receipts requirement with respect to the CFPB’s and FTC’s enforcement powers under FCRA.

Conclusion

Companies that collect and sell consumer data must be aware of and follow closely the actions taken by the FTC and CFPB. As was made clear in the *Spokeo* case and the app warning letters, the FTC will not hesitate, and, in fact, intends to treat companies in this industry as CRAs and hold them responsible for compliance with the FCRA. However, it is important to note that Spokeo may have determined its own fate by targeting professionals who were likely to use such information for the purposes covered by the FCRA, and advertising its data for purposes expressly covered by the FCRA. Had Spokeo not marketed its data in this fashion, it may have avoided regulatory action. Companies must therefore be careful about how and to whom they market their products, lest they attract the attention of regulators charged with enforcing the FCRA.

Even if data brokers adopt and implement procedures to avoid being considered a CRA, such efforts will not necessarily keep the regulators at bay. As made clear by Commissioner Brill’s comments earlier this year and most recently in the *New York Times*, the data broker industry is very much on the FTC’s radar, and although there are currently no specific laws governing this area, they may not be far off. Further, and more importantly, regulators have charged the industry with developing greater transparency in their data collection and use practices and allowing more consumer control over their information.