

FAIR CREDIT REPORTING ACT IS APPLIED TO DATA BROKER SELLING PERSONAL INFORMATION GLEANED FROM SOCIAL MEDIA FOR EMPLOYMENT SCREENING

By Scott J. Wenner

In what the Federal Trade Commission (“FTC”) touts as “the first Commission case to address the sale of Internet and social media data in the employment screening context,” Spokeo, an on-line data broker, has agreed to settle charges by the FTC that its practices violated the Fair Credit Reporting Act (“FCRA”). Signing a consent decree endorsed on June 19 in the U.S. District Court in Los Angeles, and without admitting any claims or their underlying facts, Spokeo agreed to pay a fine of \$800,000 and submit to injunctive relief chiefly aimed at compliance with the FCRA in the future.

The Fair Credit Reporting Act

The FCRA was enacted more than 40 years ago to regulate the practices of credit reporting agencies to require accuracy and privacy in assembling personal information on consumers and reporting that information in so-called “consumer reports” to users of that data.¹ The law was extensively amended in the 1990s to impose reporting and disclosure requirements for users of consumer reports and the consumer reporting agencies (“CRA”) that assemble and report the information reported. For employers, these mandates as a general matter imposed specific notice and authorization requirements on use of consumer reports which continue to apply, *e.g.*, whenever an employer retains a third party to screen an applicant for employment or conduct a background check or an investigation of a current employee. The FCRA requires credit reporting agencies that obtain and assemble the information presented

in consumer reports, in turn, to adhere to “reasonable procedures” to protect the confidentiality and ensure the accuracy and relevancy of the information that they report and to respond to assertions by consumers that information in a report is inaccurate — among other obligations.²

Employers today are familiar with the FCRA (as supplemented by the laws of certain states) as synonymous with employment screening and background checks. They tend to turn to well-established credit reporting agencies that are familiar with FCRA obligations and processes to handle employment screenings. The emergence of on-line data brokers coupled with the explosion of information that can be mined from relatively new social networks has created new challenges for employers and regulators alike in trying to apply “old” laws to new technologies and the businesses built around them. The *Spokeo* case is an example of regulators catching up.

The FTC Claims Against Spokeo

Spokeo is a privately held company headquartered in California. While it presently describes itself as a people search engine that does not permit its use for employment screenings or any other purpose covered by the Fair Credit Reporting Act, the FTC complaint quotes from materials prepared by Spokeo to describe its business differently. It states:

Spokeo assembles consumer information from “hundreds of online and offline sources,” such as social networking sites, data brokers, and other sources to create consumer profiles, which Defendant promotes as “coherent people profiles” and “powerful intelligence.” These consumer profiles identify specific individuals and display such information as the individual’s physical address, phone number, marital status, age range, or email address. Spokeo profiles are further organized by descriptive headers denoting, among other things, a person’s hobbies, ethnic-

1. “Consumer report” is broadly defined in the current law to include virtually any information collected that may be used as a factor in making a decision to extend credit or involving employment.

2. The obligations of credit reporting agencies are codified in “Fair Information Practices” — a set of rights that data subjects are given which include a right to accurate data, a right to notice when data is the basis for an adverse decision, and a right that data will be used for limited purposes.

(continued from page 1)

ity, religion, or participation on social networking sites, and may contain photos or other information, such as economic health graphics, that Spokeo attributes to a particular individual.

U.S. v. Spokeo, Inc., No. 2:12-cv-05001(C.D. Cal.), Complaint, ¶9. According to the FTC, Spokeo sells the profiles it assembles through paid subscriptions which provide a fixed number of searches and through Application Program Interfaces that provide customized and/or higher volume access. *Id.*

The FTC specifically alleged that Spokeo offered these profiles to HR, recruiting, and screening businesses as information they could use in deciding whether to interview a candidate or hire a candidate after a job interview, adding that it had agreements with high volume users specifically in HR-related fields. Spokeo's advertising and marketing efforts purportedly promoted its profiles for use in employment decision-making processes and were directed at HR, recruitment, and screening users. Its website had a tab for a page specifically for recruiters and potential customers were enticed to "Explore Beyond the Resume." *Complaint*, ¶10.³

Based on its factual allegations the FTC asserted that Spokeo was a CRA under the FCRA. The agency then claimed that Spokeo violated the FCRA by neglecting its duties as a CRA to (i) obtain basic information about data users and their certification of the purpose for which the information was being obtained; (ii) ensure that the consumer reports it sold were used for permissible purposes under the FCRA; (iii) ensure the accuracy of the information it sold; and (iv) provide users with the "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA" to inform Spokeo's customers of their FCRA obligations to data subjects.

Significance of Spokeo Issues to Employers

Spokeo is significant on two primary levels. First, on a practical level — and if there ever was any real doubt — the case confirms that the FCRA, with all of its associated notices, authorizations and processes, applies to profiling by data brokers and other third parties that is collected from social media sources and is provided for a purpose covered by the FCRA. This includes background checks and screenings as well as for

3. The FTC added that in 2010 Spokeo posted a disclaimer that prohibited users from accessing the site's information for purposes governed by the FCRA, but did nothing to limit or inhibit its then-current users from using the site for FCRA-covered purposes.

any other decision-making purposes arising in the workplace. Therefore, if employers and their third party providers comply with the FCRA, or if the employer's HR department prepares its own profile of an applicant or employee, nothing in the FCRA limits the inclusion of information gleaned from social media sites in the decision-making process of a workplace. Of course, federal and state employment discrimination laws make it risky for an employer to even have access to certain information that abounds on social media, including religious affiliation, sexual orientation, national origin, and protected activities. Access to that kind of information would effectively place a burden on employers to *disprove* that it was a factor in a decision. Beyond employment discrimination laws, some states recognize largely common law privacy rights that could be violated by unreasonable social media searches and many states have statutes that protect an employee's right to freely engage in political and other associational activities. Social media searches easily could uncover such activities and again require an employer to disprove that it was a factor in making an adverse decision.

Further, the very nature of a background check that uses social media raises questions over whether compliance with the FCRA is even possible in many instances. To be compliant, a CRA must take reasonable steps to assure the accuracy of the information it reports. Satisfying this reliability requirement seems particularly daunting in view of the casual nature of much of what is found on many social media sites.

On a different level, the FTC's action against Spokeo illustrates some of the risks associated with aggressive employment screening using social media and other available technologies never envisioned when the FCRA was amended to cover employment. As lawmakers come to grips with the vast array of data that data brokers and other "non-traditional" consumer reporting agencies can make available to employers, one can anticipate enactment of new workplace laws to catch up with today's technology. This process has begun already on a patchwork basis in reaction to publicity over abusive practices reportedly engaged in by some employers. Thus, after news reports that a few employers had demanded Facebook passwords from employees, Senator Richard Blumenthal drafted and introduced the Password Protection Act, Maryland enacted a law prohibiting the practice by employers and legislators in a number of other states, including California, introduced similar legislation.

Employers should anticipate that the FTC's action with respect to Spokeo will not be that agency's only effort to reign

(continued on page 3)

(continued from page 2)

in practices using new technologies that violate the FCRA, whether or not the practice is engaged in by a traditional CRA or a newer kind of organization such as a data broker, data aggregator, or the like. Indeed, while the FTC's action against Spokeo did not charge any employer, recruiter, or other user of the personal background data with wrongdoing, the allegations in the complaint suggest that they could have been charged.⁴ A still greater liability risk comes not from the FTC but instead from private litigation. Each negligent violation of the FCRA subjects the employer to liability for the employee's actual damages, costs of suit, and attorneys' fees. A willful violation⁵ allows each claimant to collect actual damages or "statutory damages" of up to \$1,000 (if actual damages cannot be proved), punitive damages, attorneys' fees and costs of suit. FCRA class actions appear to have been filed at a greater rate in the past 18 months because these claims are seen as well suited for class action treatment in instances where they challenge an employer's policy or repeated practice.

Regardless of whether through an FTC suit or a private class action, a significant reputational risk is presented by a challenge to an employer's use of employment screens and background checks conducted by means that include review of social media — especially if conducted by an entity that either lacks experience with or interest in FCRA compliance. Considering the kind of information available about a person from social networking sites, and from the Internet in general

-
4. If, for example, a subscribing employer or recruiter did not understand that a data broker was simply a different form of CRA and failed to obtain authorization or provide the requisite notice of rights, each applicant whose background was checked would have a claim against the employer. The claims would be sufficiently similar that if enough applicants were affected a class action could be brought. The fact that unlike established, compliant CRAs, Spokeo reportedly never sought or obtained certification of intended use from any customer or provided the requisite notices to users of their obligations makes it likely that a substantial percentage of Spokeo's customers failed to adhere to their own FCRA obligations.
 5. To be willful, a violation must be knowing or reckless; whether the employer subjectively knows it is violating the FCRA is not material. See, *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 57–58 (2007). To be reckless, the employer's "action entail[ed] 'an unjustifiably high risk of harm that is either known or so obvious that it should be known.'" *Id.*

— which could include all manner of photographs, political opinions and activity, reference to friends, relatives, romantic and/or sexual relationships, and innumerable other forms of personal information, some of which may be many years out of date, with no relationship to employment or the position sought — publicity that an employer's receipt of reports containing this kind of information is under challenge could damage that employer's reputation considerably. As noted earlier, media reports on and political reaction to overly intrusive practices have been uniformly hostile.

Conclusion

The use of social media in employment-related background checks raises new questions that are complicated by the likelihood that governing legal standards will change. Because of the risks implicated by a mistake, employers would be well advised to proceed cautiously in selecting a CRA to perform any background checks, much less those using social media. In addition, they should limit the information reported by the CRA to that which is job-related and factual, and should carefully follow all procedures and provide all notifications required by the FCRA. Further, close attention to developments relating to inclusion of social media data in background checks conducted for employment purposes is essential. ♦

This summary of legal issues is published for informational purposes only. It does not dispense legal advice or create an attorney-client relationship with those who read it. Readers should obtain professional legal advice before taking any legal action.

For more information about Schnader's Labor and Employment Practices Group or to speak with a member of the Firm at a particular Schnader office location, please contact:

Scott J. Wenner, Chair
212-973-8115; 415-364-6705
swenner@schnader.com

Michael J. Wietrzykowski, Vice Chair
856-482-5723; 215-751-2823
mwietrzykowski@schnader.com

www.schnader.com

©2012 Schnader Harrison Segal & Lewis LLP