
PUBLIC POLICY BRIEF

How the FCRA Protects the Public

DECEMBER 2013

**Software & Information
Industry Association**
www.siiia.net



DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

Copyright © 2013. All rights reserved.

Introduction

Policymakers in Congress and the FTC have been examining the business practices of information service providers seeking to understand how they acquire and use personal information in the course of their business activities. These companies, often called “data brokers,” provide information, data, and analytics to business customers in a variety of sectors to improve risk analysis and business decision-making. The information is drawn from a wide range of sources, including public records, and it is then combined with analytical capabilities to generate insight for a wide variety of business purposes.

The Fair Credit Reporting Act (FCRA), considered by many to be the first and most comprehensive federal privacy law, provides a comprehensive set of rights and responsibilities for the use of information in wide variety of contexts. It was passed in 1970 and has been updated several times. It has proven a remarkably flexible instrument that adapts to new technologies, platforms and business models. In particular, it has explicitly been adapted to deal with the gathering of information from various Internet sources such as social networks and the use of information in the context of mobile applications. This policy brief examines the extent of these protections, and it suggests that many of the harms some policymakers and commentators are discussing in the context of the use of information are addressed by the FCRA.

The FCRA illustrates a policy approach to protecting people from harm that could result from the misuse of personal information that is somewhat at variance from the standard notice and choice framework of privacy regulation. Instead of simply describing information use (that is, giving notice) and providing consumer choice, the “harm framework” seeks to identify the likely harms that the activities of these companies might cause, and then target any needed regulatory interventions to mitigate or reduce the risks of harm in a way that balances the costs and benefits involved.¹

Consumer Reporting Agencies Under the FCRA

Information service providers are essential actors in today's data-driven economy. They collect, aggregate, link and analyze information in ways that are vital to economic growth, innovation, job creation and international competitiveness.

Although the technology has improved, the use of information to improve business decisions is not new. A generation ago, Congress recognized that this use of information was both essential to economic growth and the smooth functioning of a modern economy, and a potential source of adverse consequences for individuals. In creating the FCRA, Congress validated this use of information and created a regulatory structure to manage the risks of harm.

The regulatory framework created by the legislation established a set of rights and responsibilities for the collection and use of personal information when used for certain specified eligibility decisions. When, in Congress's judgment, information was used in ways that risked substantially affecting a person's life chances in a negative way, it was brought under this regulatory framework. Other uses of information were left outside of this framework.

The FCRA applies to consumer reporting agencies, which are defined as:

... any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.²

The FCRA defines a consumer report as:

... any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose under Section 604 [15 U.S.C. § 1681b].³

The "other purposes" listed in Section 604 include insurance for the consumer, eligibility for a government benefit, assessment of a consumer's existing credit risk by potential investor or servicer of an existing consumer debt and a "legitimate business need" in connection with a transaction initiated by the consumer. This last concept of legitimate business need is subject to substantial interpretation by courts and the FTC, and is potentially quite broad.⁴

The FCRA sets out a series of rights and obligations to protect consumers, including requirements for disclosure and notice of adverse action, consent for sharing information with employers, access and correction requirements, and use limitations.⁵

More specifically, the FCRA sets out the following rights and obligations regarding consumer reporting agencies:

- **Notice of Adverse Action:** People must be told if information in a consumer report has been used against them. If they have been denied credit, insurance or employment, for instance, they must be informed of this adverse action.
- **Disclosure:** People have the right to know what is in their file. In many cases, people are entitled to free access to their file such as when adverse action occurs, and also have a right to one free disclosure annually. People have the right to ask for a credit score.
- **Access and Correction:** People have the right to dispute incomplete or inaccurate information and credit reporting agencies have an obligation to correct or delete inaccurate, incomplete, or unverifiable information.
- **Use Limitations:** A consumer reporting agency may provide information about data subject only to companies or individuals with a valid need such as to consider an application with a creditor, insurer, employer, or landlord. Moreover, consumer reporting agencies may not report outdated negative information such as negative information that is more than seven years old, or bankruptcies that are more than 10 years old.
- **Consent:** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. People have a right to opt-out of unsolicited “prescreened” offers for credit and insurance. Consumers do not have the right to limit the collection of information, since this kind of consent would allow the bad risks to opt out of the system, thereby reducing its usefulness.
- **Redress:** People may sue in state or federal court and seek damages from those who violate the FCRA, including consumer reporting agencies, or, in some cases, users of consumer reports or furnishers of information to a consumer reporting agency. This system was updated several times since its establishment in the 1970s to take into account new business practices and technological changes. But the basic structure remains in place and has proven to be a balanced and effective regulatory regime that allows for industry growth and innovation while narrowing and reducing the risks of harmful effects on individuals.

Furnishers of Information Under the FCRA

Companies that provide information to consumer reporting companies are also regulated under the FCRA. They are called furnishers, a term defined in the statute as “an entity that furnishes information relating to consumers to one or more consumer reporting agencies for inclusion in a consumer report.”⁶ They have their own set of responsibilities under the FCRA, including general legal duties to provide accurate information and to investigate the accuracy of information upon notification of a dispute. More specifically these responsibilities include:⁷

- **A prohibition on providing inaccurate information.** This includes reporting information with actual knowledge of errors and reporting information after notice and confirmation of errors.
- **Duty to correct and update information.** Once a furnisher determines that information is not complete or accurate, it must promptly notify consumer reporting companies, provide corrected information and refrain from furnishing the inaccurate or incomplete information.
- **Duty to provide notice of dispute.** If a consumer disputes the accuracy or completeness of information, the furnisher must not provide the disputed information to a credit reporting company without a notice of this dispute.
- **Duties regarding notice of closed or delinquent accounts.** Furnishers must provide credit reporting agencies with notice when a consumer closes a credit account. If they report delinquent accounts, they are subject to restrictions on timing and sourcing of these delinquency notices.
- **Duties related to identity theft information.** Furnishers have to have reasonable procedures in place to respond to notices from consumer reporting agencies relating to identity theft information to block the resubmission of that information. If the furnisher receives an identity theft report from a consumer, it may not furnish that information to a consumer reporting agency unless it subsequently knows or is informed by the consumer that the information is accurate.
- **Duty to notify consumer when upon furnishing negative information.** Furnishers that extend credit must have in place reasonable policies and procedures to notify consumers when they provide negative information to consumer reporting agencies.
- **Duty to Reinvestigate Disputed Information.** Based on a direct request of a consumer, furnishers are generally required to reinvestigate a dispute concerning the accuracy of information contained in a consumer report on the consumer, to report the results of that investigation to the consumer and to notify consumer reporting agencies if it finds that the information furnished is inaccurate.
- **Accuracy Guidelines.** Furnishers are subject to regulatory guidelines regarding the accuracy and integrity of the information relating to consumers that such entities furnish to consumer reporting agencies. They must establish policies and procedures for implementing these guidelines.⁸

A distinctive feature of the FCRA is its limited role for consent. It does not provide consumers with a right to block the flow of information to consumer reporting agencies. Under the FCRA, consumer reporting agencies can use information only for permissible purposes and they face substantial duties to maintain accuracy and correct mistakes, but consumers have no right to stop them from gathering information relating to them. The reason is straightforward. Consumer reporting agencies gather information about individuals in order to assess their suitability for insurance, credit access, employment and other benefits. Their reports contain both positive and negative information about people, and they provide users of consumer reports with the ability to assess the risk involved in

making people eligible for these benefits. If people who are bad risks were able to withhold information from these agencies, the files would lose a large part of their value for critical risk analysis purposes.⁹

Applying the FCRA in the 21st Century

Decades of FTC enforcement action, interpretation and court decisions under the FCRA have established a set of business practices that generally vindicate the interests of consumers in protection from the harmful use of information in a wide range of eligibility contexts. It has been updated several times.¹⁰

It might seem, however, that such a legal framework, put in place to deal with the information service providers of the 1970s, cannot possibly have the resources to address concerns some policymakers have about “data brokers” in the 21st century. Nevertheless, the FTC has successfully applied the FCRA rules in a number of recent cases to business ventures using the most advanced, technologically up-to-date techniques of data collection and analysis. A number of examples illustrate the point that the FCRA is applicable to a wide range of contemporary data collection and uses.

Applying the FCRA to Online Data Collection – The Case of Spokeo

Traditional consumer reporting agencies gathered information directly from furnishers. But does the FCRA apply to companies that gather publicly available information online and make it available to others for eligibility decisions? The FTC ruled in the case of Spokeo that online data aggregators are covered under the FCRA when they make profiles available to third-parties for FCRA-regulated purposes.

Founded in 2006, Spokeo collected personal information about consumers from hundreds of online and offline data sources, including social networks. It merged the data to create detailed personal profiles of consumers containing a broad range of personal information including name, address, age range, email address, hobbies, ethnicity, religion, participation on social networking sites, and photos. It also offered credit, wealth and lifestyle data. Initially, the site was marketed to employers and other decision-makers who were encouraged to rely on the advertised credit, wealth and lifestyle data to make eligibility judgments about consumers.

In June 2010, the Center for Democracy and Technology filed a complaint against Spokeo with the FTC, asking the agency to bring companies like Spokeo, that provide online information to companies for making eligibility decisions, under the scope of the FCRA.¹¹

In June 2012, the FTC fined Spokeo for improperly marketing consumer information profiles to companies in the human resources, background screening, and recruiting industries without taking steps to protect consumers required under the FCRA. In particular, the

agency said that Spokeo failed to maintain reasonable procedures to verify who its users are and that the consumer report information would be used for a permissible purpose; to ensure accuracy of consumer reports; and to provide notice to the covered consumer when someone purchased its consumer reports.¹²

Partly as a result of this decision, Spokeo has withdrawn from the consumer reporting business. It now clearly states that it is not a consumer reporting agency and that its information is not to be used for any FCRA-regulated purpose.¹³

Applying the FCRA to Social Media – The Case of Social Intelligence

Despite the Spokeo example, the FCRA rules do not act as a ban on new technology or the innovative use of information to aide in business decision-making. All they do is make sure that any company must provide reasonable consumer protections when they use information for sensitive eligibility decisions that can affect people's life chances. The case of Social Intelligence illustrates this point.

Social Intelligence is an Internet and social media screening company. It automates the collection of data from social networks and other online sources as inputs into employment decisions. It searches social networks, blog entries, videos, photos, comments, and other forms of user-generated content available publicly on the Internet. Then it collects, verifies, analyzes, and identifies information about a job candidate. It does not provide "protected class" information to employers such as race, color, religion, sex, national origin, age, gender identity, disability status, veteran status, and genetic information. It uses legally permitted employer-defined criteria to compile reports on potential employees.¹⁴

This innovative company that uses the most up-to-date data collection and analytic techniques is a consumer reporting agency under the FCRA. It furnishes consumer reports that are used by third parties as a factor to determine eligibility for employment. It clearly states that in doing this, it maintains, "reasonable procedures designed to ensure that the consumer report is only used for permissible purposes, require employers to obtain signed Disclosure and Authorization forms from the individuals to be background checked, ensure employers follow FCRA Adverse Action procedures, and have a complete dispute resolution process."¹⁵ After an investigation, the FTC concluded that the company's policies and procedures did not require any further action to assure compliance with the FCRA's requirements.¹⁶

Applying the FCRA to Mobile Apps – The Case of Filiquarian Publishing

In early 2012, the FTC demonstrated that the FCRA also effectively operates in the world of mobile applications, issuing warning letters to providers of six mobile applications that

provided background-screening services that they may be violating the FCRA. The FTC warned the application providers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the Act.¹⁷ The FTC followed up in 2013 by bringing a case against Filiquarian Publishing that established its policy in the application of the FCRA to mobile apps.¹⁸

In this case, the FTC concluded that a mobile app company is a “consumer reporting agency” under the FCRA if it assembles reports containing information relating to a person’s character, reputation, or personal characteristics for the purpose of providing those reports to third parties who use them or are expected to use them for eligibility decisions relating to employment, housing, credit, insurance or the like. A mobile app provider cannot escape FCRA obligations just by asserting that it is not a consumer reporting agency if it has good reason to believe that its reports are being used for these purposes.

Marketing Information Service Providers

Companies sometimes want to pursue economically beneficial uses of information in ways that do not involve specific harmful uses of that information to individuals. They often consciously design their programs to avoid the uses of information that would be covered by the FCRA and take steps to reassure their customers through public commitments to restrict their use of information. Spokeo chose this strategy, following its settlement with the FTC. The marketing industry as a whole has done so as well.

Marketing companies gather information from a wide variety of public and private sources. They analyze it and make it available to their business customers for the purpose of allowing them to reach people who might be interested in purchasing their products and services. With companies in every sector relying on marketing data to reach their customers effectively, the value of marketing services to the economy is enormous, adding \$156 billion in revenue to the U.S. economy and fueling more than 675,000 jobs in 2012 alone.¹⁹

Information aggregators in the marketing industry gather information to enable companies to reach an audience with a description of products and services that might interest them. They do not want their information to be used for eligibility decisions, but rather to inform companies to reach their intended audience with relevant marketing messages. The self-regulatory policies of the marketing industry are designed to publicize and enforce this industry’s self-imposed limitations on the use of marketing data base to purely marketing purposes.²⁰ Marketing is not an activity covered under the FCRA and so these industry limitations ensure that companies gathering information for marketing purposes will not be covered under FCRA.

The policy of including uses of information for many eligibility determinations under FCRA, while keeping marketing uses out of that framework is well established and is proportional on the basis of the different harms that could befall people under the different uses. Eligibility decisions directly affect consumers’ life chances and prospects. Applying for a home loan, for instance, is often the most important financial decision that families make. Marketing,

however, does not have such an effect on people's life chances. It is merely a way in which companies decide to whom they should direct their messages. People have other ways to reach out to companies to learn their true options – through easily available Internet channels and advertising that are not specific to particular individuals.

Conclusion

Public policy is in a state of flux as the new techniques of data collection and analysis diffuse through society and the economy.²¹ It is crucial that we establish and maintain a public policy framework so that the protection of individual privacy can complement rather than thwart the natural evolution of these techniques. We can have good privacy protection as well as innovation and economic growth. Despite its lineage that is ancient in technology terms--dating from 1970--the FCRA has proven capable of providing good privacy protection and operating space for a wide variety of information uses that employ the latest techniques of data collection and analysis. Indeed, the recent actions by the FTC demonstrate the broad coverage of the FCRA to innovative information service providers never imagined when the law was enacted. This FCRA framework, which focuses on the harm that could adversely affect the life chances of people rather than notice and choice, is a good model for how to think about privacy policy in the age of data-driven innovation.

Endnotes

1. J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information 75 U. Chi. L. Rev. 109 2008 pp. 109-120
2. 15 U.S.C. § 1681a(f)
3. 15 U.S.C. §1681a(d)(1)
4. 15 U.S.C. §1681b(a)(3)
5. <http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>
6. 12 CFR 334.41
7. 15 USC § 1681s-2
8. See Appendix A Part 660—Interagency Guidelines Concerning the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies at <http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=89d50ede6e4072bde4d4a944a89bd200&rgn=div5&view=text&node=16:1.0.1.6.77&idno=16#16:1.0.1.6.77.0.39.5.48>
9. Beales and Muris Choice or Consequences, pp. 116-117
10. The latest major amendments were the Fair and Accurate Credit Transaction Act of 2003, Pub.L. 108–159 at <http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/html/PLAW-108publ159.htm>
11. Press Release from CDT, Center for Democracy and Technology Files FTC Complaint Against Spokeo, Inc. (June 30, 2010) at http://www.cdt.org/pr_statement/center-democracy-and-technology-files-ftc-complaint-against-spokeo-inc
12. <http://www.ftc.gov/opa/2012/06/spokeo.shtm>.
13. <http://www.spokeo.com/about>
14. <http://www.socialintel.com/index.php/faqs>
15. <http://www.socialintel.com/index.php/faqs>
16. Letter to Renee Jackson, Counsel for Social Intelligence Corporation, May 9, 2011 at <http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/social-intelligence-corporation>

17. <http://www.ftc.gov/news-events/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting>
18. <http://www.business.ftc.gov/blog/2013/01/background-screening-reports-and-fcra-just-saying-youre-not-consumer-reporting-agency-i>
19. The Value of Data: Consequences for Insight, Innovation, and Efficiency in the U. S. Economy, " A Study Commissioned by DMA's Data Driven Marketing Institute (DDMI) October 14, 2013 <http://ddminstitute.thedma.org/files/2013/10/DDMI-Summary-Analysis-Value-of-Data-Study.pdf>
20. http://www.the-dma.org/nonprofitfederation/NP_Annotated_Ethical_Guidelines.pdf
21. SIIA, Data Driven Innovation: Understanding and Enabling the Economic and Social Value of Data, May 2013 at http://siaa.net/index.php?option=com_content&view=article&id=1293:data-driven-innovation&catid=163:public-policy-articles&Itemid=1411