Regulatory Compliance Review

CONSUMER PRIVACY AND CONFIDENTIALITY

By Jonathan Foxx

Last month, I discussed the announcement made by the Consumer Financial Protection Bureau (CFPB) regarding the confidential treatment of information obtained from persons in connection with its exercise of authorities under federal consumer financial law.[1] I offered an Action Plan that a financial institution, bank or non-bank, should implement in preparation for a CFPB examination, with respect to protecting the confidentiality and privilege of documents and information.

This month, I would like to discuss new consumer privacy protection updates at the Federal Trade Commission (FTC), the watchdog enforcement agency charged with protecting consumer privacy, as the FTC has issued sweeping revisions to its privacy rules. In this article, we will take a look at the FTC's call for companies to adopt best privacy practices.

These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency.

Overview

On March 26, 2012, the FTC issued a final report of 112 pages, setting forth best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data.

In the report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," the FTC also recommends that Congress consider enacting general privacy legislation, data security and breach notification legislation, and data broker legislation.[2]

The Report follows a preliminary staff report that the FTC issued in December 2010. The preliminary Report proposed a framework for protecting consumer privacy with respect to the new communication technologies of this century.

Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated nearly 40 years ago:

- Privacy by design: Build in privacy at every stage of product development.
- Simplified choice for businesses and consumers: Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do-Not-Track mechanism, while reducing the burden on businesses of providing unnecessary choices.
- Greater transparency: Make information collection and use practices transparent.

Privacy by design

Companies should build in consumers' privacy protections at every stage in developing their products. These include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy.

Simplified choices for businesses and consumers

Companies should give consumers the option to decide what information is shared about them, and with whom. This should include a Do-Not-Track mechanism that would provide a simple, easy way for consumers to control the tracking of their online activities.

Greater transparency

Companies should disclose details about their collection and use of consumers' information, and provide consumers access to the data collected about them.

What has changed?

The Report changes the guidance's scope; that is, the preliminary report of December 2010 recommended that the proposed framework apply to all commercial entities that collect or use consumer data that can be linked to a specific consumer, computer or other device, but now, this final Report concludes that the framework should not apply to companies that collect and do not transfer only non-sensitive data from fewer than 5,000 consumers a year.

The Report also responds to comments filed by organizations and individuals that, with technological advances, more and more data could be "reasonably linked" to consumers, computers or devices. Thus, the Report concludes that data is not "reasonably linked" if a company takes reasonable measures to re-identify the data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it.

Furthermore, the Report refines the guidance for when companies should provide consumers with choice about how their data is used.

It states that whether a practice should include choice depends on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business or is required or specifically authorized by law. These practices would include product fulfillment and fraud prevention.

Finally, the Report contains important recommendations regarding data brokers. It notes that data brokers often buy, compile, and sell highly personal information about consumers. The FTC observes that consumers are often unaware of their existence and the purposes to which they use the data.

Therefore, the Report makes two recommendations to increase the transparency of such data broker practices by first reiterating the FTC's prior support for legislation that would provide consumers with access to information held by data brokers, and, secondly, by calling on data brokers who compile consumer data for marketing purposes to explore the creation of a centralized website where consumers could get information about their practices and their options for controlling data use.

Future issues

Over the course of the next year, the FTC has stated that it will work to encourage consumer privacy protections by focusing on five (5) main action items:

- Do-Not-Track
  The FTC commends the progress made in this area: browser vendors have developed tools to allow consumers to limit data collection about them, the Digital Advertising Alliance has developed its own icon-based system and also committed to honor the browser tools, and the World Wide Web Consortium standards-setting body is developing standards.

- Mobile
  The FTC urges companies offering mobile services to work toward improved privacy protections, including disclosures. To that end, it will host a workshop on May 30, 2012 to address how mobile privacy disclosures can be short, effective and accessible to consumers on small screens.

- Data brokers
  The FTC will call on data brokers to make their operations more transparent by creating a centralized website to identify themselves, and to disclose how they collect and use consumer data. In addition, the website should detail the choices that data brokers provide consumers about their own information.

- Large platform providers
  The Report cited heightened privacy concerns about the extent to which platforms, such as Internet Service Providers (ISPs), operating systems, browsers and social media companies, seek to comprehensively track consumers' online activities. The FTC will host a public workshop in the second half of 2012 to explore issues related to comprehensive tracking.

- Promoting enforceable self-regulatory codes
  The FTC will work with the Department of Commerce and stakeholders to develop industry-specific codes of conduct. To the extent that strong privacy codes are developed, when companies adhere to these codes, the FTC will take that into account in its law enforcement efforts. If companies do not honor the codes they sign up for, they could be subject to FTC enforcement actions.

Jonathan Foxx, former chief compliance officer for two of the country's top publicly-traded residential mortgage loan originators, is the president and managing director of Lenders Compliance Group, a mortgage risk management firm devoted to providing regulatory compliance advice and counsel to the mortgage industry. He may be contacted at (516) 442-3456 or by e-mail at jfoxx@lenderscompliancegroup.com.

Footnotes

1—Foxx, Jonathan, Regulatory Compliance Review: The CFPB's Treatment of Confidentiality and Privilege, National Mortgage Professional Magazine, *April 2012, Volume 4, Number 4, pages 30-31.*

2—Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Recommendations for Businesses and Policymakers, Federal Trade Commission, March 2012.