MORRISON | FOERSTER

Morrison & Foerster Client Alert.

April 3, 2012

FTC Releases Final Privacy Report Outlining Best Practices and Expressing Support for Baseline Privacy Legislation

By Julie O'Neill, Reed Freeman, and Nicholas Datlowe

On March 26, 2012, the Federal Trade Commission (the "Commission" or "FTC") released its much-anticipated final privacy report, *Protecting Consumer Privacy in an Era of Rapid Change*.[1] The report builds upon the preliminary report released by the Commission in December 2010,[2] and it provides recommendations for businesses and policymakers with respect to online and offline privacy practices. Specifically, the report:

- **Presents a privacy framework that sets forth best practices – not legal requirements – for businesses.** The Commission makes it clear that, to the extent that the best practices set forth in the report extend beyond existing legal requirements, they are not intended to serve as a template for law enforcement actions or regulation under laws currently enforced by the Commission. FTC Chairman Jon Leibowitz reiterated this point to a House Energy and Commerce subcommittee on March 29, 2012, telling legislators that, while companies that follow the report's best practices would not be in violation of the FTC Act, those that do not follow them would not necessarily be in breach of the law. In his words, the report "is not a regulatory document or an enforcement document." That said, those elements of the report that focus on transparency and consumer choice build on the Commission's recent law enforcement experience. It is therefore reasonable to assume that the Commission will continue its pattern of focusing on data practices that are not obvious to consumers in context, that are not disclosed adequately, and, in some instances, where consumers do not have meaningful choice. Of course, the Commission will continue its aggressive enforcement of companies' privacy and data security promises.

- **Recommends baseline privacy legislation.** In the Commission's view, because self-regulation has not yet gone far enough, flexible and technologically neutral baseline privacy legislation is desirable. While encouraging industry to continue its self-regulatory efforts, the Commission also intends the privacy framework set forth in the report to assist Congress in crafting legislation. The Commission also reiterates its call for federal information security and data breach notification legislation and for legislation regulating the practices of data brokers.

[1] The final report is available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[2] The preliminary report is available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. *See also* http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf.

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Olivier Proust 32 2 340 7360
Karin Retzer 32 2 340 7364

Hong Kong
Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

- **Highlights the Commission's privacy priorities for the coming year.** The report explains that the Commission will promote implementation of the privacy framework by focusing its efforts in five main areas: (1) cooperation with industry to complete the implementation of an easy-to-use, persistent, and effective ***Do Not Track*** mechanism (the Commission does *not* call for Do Not Track legislation in this report); (2) improvement of privacy disclosures and other protections offered by ***mobile services***, including through its May 30, 2012 public workshop on revisions to its Dot Com Disclosures guidance;[3] (3) support for targeted legislation to give consumers access to the information about them held by ***data brokers*** and encouragement to data brokers that compile data for marketing purposes to create a centralized website to further increase the transparency of their practices;[4] (4) exploration of the privacy issues associated with the comprehensive tracking of consumers' online activities by ***large platform providers***, such as ISPs, operating systems, browsers, and social media in a workshop later this year; and (5) participation with the Department of Commerce and industry stakeholders to create ***enforceable self-regulatory codes of conduct***.

This final priority reflects the Commission's support for the report issued by the Administration on February 23, 2012. In its report, entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*,[5] the Obama administration detailed a "Consumer Privacy Bill of Rights" and announced the creation of a multistakeholder process to be convened by the Department of Commerce to create voluntary codes of conduct which, if adopted by companies, would be enforceable by the Commission pursuant to its deception authority under Section 5 of the FTC Act. **Importantly, the Commission's report makes clear that the FTC will participate in the Department of Commerce's multistakeholder process.**

THE SCOPE OF THE PRIVACY FRAMEWORK

The privacy framework applies to all commercial entities that collect or use online and/or offline consumer data that can be reasonably linked to a specific consumer or computer or other device. There is an exception for entities that collect only non-sensitive data from fewer than 5,000 consumers per year and do not share the data with third parties, so as not to unduly burden small businesses.[6] The Commission did not, however, exempt from the framework's intended coverage those companies already covered by sector-specific privacy laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. Instead, it emphasizes in the final report that the framework is intended to foster best practices but not impose conflicting legal obligations.[7]

The extension of privacy best practices to data linkable to a computer or other device reflects the Commission's position that the line between "personally identifiable information" ("PII") and "non-PII" is increasingly blurred. The Commission justified this application on the grounds that, not only is re-identification of supposedly "anonymous" data increasingly possible, but, in the Commission's view, businesses have strong incentives to re-identify such data.

To provide businesses with certainty with respect to what constitutes "reasonably linkable" data, the Commission has taken the position that data is not "reasonably linkable"—and therefore not within the scope of the privacy framework—if the company possessing it implements the following protections: (1) reasonable measures to ensure that the data is

[3] *See* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[4] The Commission proposes that such a website would: (1) identify data brokers to consumers and describe how they collect and use consumer data; and (2) detail the access rights and other choices the data brokers provide with respect to the data they maintain.

[5] The Administration's report is available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[6] "Sensitive data" includes Social Security numbers and financial, health, children's, and geolocation information.

[7] The Commission urges Congress not to pass legislation that creates overlapping or contradictory requirements for entities subject to existing sector-specific privacy laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act.

de-identified; (2) a public commitment to using the data in a de-identified way; and (3) contractual prohibitions on downstream entities that use the data from de-identifying it, coupled with reasonable measures to ensure compliance with that prohibition. Even with this attempt at clarity, questions remain, including what it means to "de-identify" data. For example, does this mean removing PII or does it mean removing any identifier, such as cookie IDs? Furthermore, what measures are "reasonable" in terms of monitoring downstream entities?

THE SUBSTANCE OF THE PRIVACY FRAMEWORK

The Commission's report proposes a privacy framework that calls for companies to incorporate "privacy by design" into their practices, to offer consumers ***simplified choice*** about how their data is collected and used, and to provide consumers with ***greater transparency*** about their practices.

Privacy by Design

According to the report, companies should promote consumer privacy throughout their organizations and at every stage of the development and life cycle of their products and services. As a substantive matter, this means that companies should incorporate the following privacy protections into their practices:

- ***Reasonable security*** for consumer data. The Commission notes that this obligation is already well settled, as it has a long history of enforcing data security obligations under Section 5 of the FTC Act and other laws. The Commission commends industry's efforts to ensure the security of consumers' data, but, nonetheless, **it renews its call for Congress to enact comprehensive data security and breach notification legislation**.
- ***Reasonable limits on data collection***. According to the Commission, reasonable limits are those that are consistent with the context of a particular transaction or the consumer's relationship with the business (or as required or specifically permitted by law).
- ***Sound retention and disposal practices***. The Commission states that companies should implement reasonable restrictions on the retention of consumer data and should dispose of it once the data has outlived the legitimate purpose for which it was collected. What is "reasonable" depends on the type of relationship and the nature and use of the data.[8]
- ***Data accuracy***. According to the Commission, companies should maintain the accuracy of the data they hold about consumers. As with other elements of the framework, the Commission believes that the best approach to achieving accuracy is through a flexible approach, scaled to the intended use and sensitivity of the data at issue.

The Commission also urges businesses to maintain comprehensive data management procedures throughout the life cycle of their products and services. It cites its recent settlement orders with Facebook[9] and Google[10] as providing a roadmap for the types of comprehensive procedural protections it envisions: (1) designation of personnel responsible for the privacy program; (2) a risk assessment that covers, at a minimum, employee training, management, and product design and development; (3) implementation of controls designed to mitigate identified risks; (4) appropriate oversight; and (5) evaluation and adjustment of the program in light of regular testing and monitoring.

[8] The Commission calls on trade associations and self-regulatory groups to provide businesses with guidance about data retention and destruction policies.

[9] *See* http://www.mofo.com/files/Uploads/Images/111208-Facebook-Proposed-Settlement.pdf.

[10] *See* http://www.mofo.com/files/Uploads/Images/110404-FTC-Privacy-Priorities.pdf.

Simplified Consumer Choice

The report encourages companies to simplify consumer choice, in part by identifying those practices for which choice is not necessary. Specifically, the report provides that **companies do not need to provide consumers with choice before collecting and using consumer data for practices that are *consistent with the context of the transaction or the company's relationship with the consumer* or that are required or specifically authorized by law**. While this standard relies to some degree on consumer expectations, it focuses on objective factors related to the consumer's relationship with the business. The following commonly accepted practices are provided as examples of the kinds of practices that do not typically require consumer choice: product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing.

The report goes on to address **practices that require choice** and says that, when choice is required, it should be offered at a time and in a context in which the consumer is making a decision about his or her data.[11] As a general matter, **data use and disclosure practices that are inconsistent with the context of the transaction or the company's relationship with the consumer require consumer choice** (unless such practices are required or specifically authorized by law). Such practices may include, for example, sharing customer data with an affiliate for the affiliate's own direct marketing use, if the consumer would not be aware of the affiliate relationship (*e.g.*, because the companies are differently branded).

The Commission identifies two practices that it believes require ***affirmative express consent***: (1) in connection with **material retroactive changes to privacy representations** (this is not new, as the Commission has expressed it repeatedly for years and has imposed it in settlement orders); and (2) **before collecting sensitive data**, such as information about children, health and financial information, geolocation data, and Social Security numbers.[12] This suggests that where the Commission otherwise calls for choice, **clear and conspicuous notice and opt-out** would be sufficient.

Greater Transparency

The Commission states that companies should increase the transparency of their data practices, through privacy notices, access to data, and consumer education:

- ***Privacy notices*** should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.[13] The Commission calls for the simplification of privacy notices, such as through the use of standardized terminology, format, and/or other elements. In the Commission's view, members of various industry sectors should work together to create standards relevant to their industry, possibly through the multistakeholder process that the Department of Commerce plans to convene.

- Companies should provide ***reasonable access*** to the consumer data they maintain. The extent of access should be proportionate to the sensitivity of the data and the nature of its use. For example, the Commission urges businesses that maintain data for marketing purposes to, at a minimum, provide consumers with access to such data and permit them to suppress categories they would not like used for targeting.

[11] Although the Commission has supported the use of "just-in-time" privacy notices and choice mechanisms, it does not impose any particular method in this report. Instead, it notes that industry sectors are well positioned to develop the choice mechanisms that are most appropriate for themselves.

[12] The Commission also proposes that social networks and others specifically targeting teens should take extra precautions with respect to their submission of personal information.

[13] According to the Commission, the need for simplification and industry involvement is particularly acute in the mobile realm, given the number of entities that want to collect user data and the limited space for disclosures. As noted above, the Commission plans to address mobile disclosures in a May 30, 2012 public workshop.

- Companies should make efforts to increase the transparency of their ***data enhancement*** practices. The Commission does not suggest that companies obtain consent to such practices; however, it urges industry to rely on the other elements of the privacy framework to address the privacy concerns raised by it. In the Commission's view, this means that companies should, for example, explain to consumers how data enhancement works and how they can contact data enhancement sources directly. They should also encourage their data sources to increase their own transparency.
- The Commission encourages companies to continue to engage in ***consumer education*** efforts and invites industry to re-brand and use the Commission's own materials.

CONCLUSION

The report reflects the Commission's continued concern that consumers bear too much of a burden for understanding and controlling how their data is collected, used, retained, and disclosed. The report reflects its desire to see this paradigm reversed so that the burden is shouldered by companies instead. How far this concern is turned into enforceable requirements will depend in large part on the support the Commission receives from Congress, as well as the extent of the development and adoption of self-regulatory codes of conduct.