December 3, 2010

FTC Releases Draft Privacy Report Outlining Best Practices, Possible New Requirements Under Section 5 of the FTC Act, and Expressing Support for a "Do Not Track" List

By Reed Freeman and Julie O'Neill

On December 1, 2010, the Federal Trade Commission (FTC or Commission), by a vote of 5-0, released its long-awaited staff report on privacy, Protecting Consumer Privacy in an Era of Rapid Change.[1]

Based largely on themes and concepts developed through a series of privacy roundtables held by the Commission over the past year, the report sets out an expansive proposed framework for how companies should protect consumers' privacy. Although the Commission set out to develop a framework for applying its existing authority under Section 5 of the FTC Act to modern privacy practices, the report falls far short of that ambition. Rather, while breathtaking in its scope and detail, it leaves more questions than answers. Most importantly, the Commission's report is long on recommendations but short on which of those recommendations amount to requirements under Section 5. Comments are due by January 31, 2011, and the Commission expects to release a final report, which may be more concrete, later in 2011.

The proposed framework embodied in the report consists of three major elements repeatedly touted by Commission officials in recent months: (1) "privacy by design," (2) simplified consumer choice, and (3) greater transparency. (We discuss each of these elements below.) That said, several key points deserve highlighting:

- **The framework covers a broad range of commercial entities**. These include those doing business *offline* as well as *online*, and including companies that process consumer data but may not interact directly with consumers (such as data brokers).

[1] The report is here: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Beijing

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

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365
Antonio Seabra Ferreira 32 2 340 7367

Hong Kong

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

Los Angeles

Mark T. Gillett (213) 892-5289
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Chris Coulter 44 20 7920 4012
Suzanne Horne 44 20 7920 4014

New York

Gabriel E. Meister (212) 468-8181
Joan P. Warrington (212) 506-7307
John F. Delaney (212) 468-8040
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Bryan Wilson (650) 813-5603
Christine E. Lyon (650) 813-5770

San Francisco

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

Tokyo

Daniel P. Levison 81 3 3214 6717
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.

Andrew M. Smith (202) 887-1558
Cynthia J. Rich (202) 778-1652
Julie O'Neill (202) 887-8764
Nathan David Taylor (202) 778-1644
Obrea O. Poindexter (202) 887-8741
Reed Freeman (202) 887-6948
Richard Fischer (202) 887-1566
Kimberly Strawbridge Robinson (202) 887 1508

- **The framework covers both personally identifiable information, as well as data that can be reasonably linked to a specific consumer, computer, or other device**. The Commission explains that this approach is supported by the fading of the traditional personally identifiable information (PII)/non-PII distinction, "due to changes in technology and the ability to re-identify consumers from supposedly anonymous data."[2]

- **The framework endorses the creation of a Do Not Track mechanism for online behavioral advertising.** Explaining that industry efforts to provide consumers with easy control over the tracking of their online activities have fallen short, the Commission "supports" a do not track mechanism as the most practical way to simplify consumer choice around online tracking.

The framework is not final. A review of the almost 80-page report reveals many specific questions on which the Commission has requested comment. It encourages interested parties – which include every company that collects or receives consumers' data – to submit comments to guide its further development and refinement of the framework. We underscore that encouragement and urge affected businesses to carefully consider the proposed framework's implications for how they collect, use, retain, and share consumer data. Comments are due to the Commission by January 31, 2011.

The Commission's proposed framework consists of three major elements: (1) privacy by design, (2) simplified consumer choice, and (3) greater transparency.

1. PRIVACY BY DESIGN

The framework proposes to make privacy and data security a routine consideration for businesses. In the Commission's view, "companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services." In practical terms, this means that a company that processes consumer data should follow a version of the fair information practices originally developed by the OECD decades ago. Collectively, these appear to be recommended best practices rather than new requirements under Section 5. Individually, however, some of these recommendations, such as reasonable security and secure disposal, are already considered by the Commission to be required under Section 5.

Elements of Privacy By Design

- **A company should incorporate substantive privacy protections into its everyday practices.** These protections include: (1) providing reasonable security for consumer data, (2) collecting only the data needed for a specific business purpose, (3) retaining data only as long as necessary to fulfill that purpose, and (4) implementing reasonable procedures to promote data accuracy.

- **A company should maintain comprehensive data management procedures throughout the life cycle of its products and services.** What does this mean? A company should develop, implement, and enforce a comprehensive privacy program, tailored in size and scope to the risks presented to the data it processes. It should also designate personnel to train employees, promote accountability, and periodically review the program. Among other things, according to the report, an appropriate program should ensure that privacy and data security are taken into account in the early stages of development and throughout the lifecycle of the resulting product or service.

This second bullet draws its inspiration from the Commission's data security cases, where Commission orders have required companies to engage in security training, designate employees responsible for an information security program,

[2] This is not the first time that the Commission has taken this position. It similarly extended the scope of its Self-Regulatory Principles for Online Behavioral Advertising to both PII and non-PII. *See* Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), pp. 20-26 (available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf) (OBA Report).

and audit their security practices over time. These concepts are new to the privacy world, at least as a legal requirement under Section 5 imposed in the U.S. across industries.

2. SIMPLIFIED CONSUMER CHOICE

The framework sets forth ways in which companies should, according to the report, make data choices more prominent, relevant, and easily accessible to consumers.

- **Choice can be implied for obvious data uses and disclosures.** When a company uses data in a way that is commonly accepted and expected by a consumer, the Commission believes that the consumer's consent to that use can reasonably be inferred. The Commission further believes that this category of uses is narrow, likely including only product and service fulfillment, internal operations, fraud prevention, legal compliance, and first-party marketing. Clearly, because this category results in implied consent, the comments are likely to focus on which types of uses are and are not "commonly accepted." Accordingly, we believe that businesses should review their data practices to determine which merit treatment as "commonly accepted" in context under this paradigm, and to make those arguments in their comments.

- **Choice must be offered for all other (non-obvious) uses and disclosures**. These include, for example, sharing data with a third party for its own marketing or other purposes and social media services where the service provider permits third party applications to collect users' data. Because these uses and disclosures are not obvious to a consumer, the Commission argues, a consumer's consent to them cannot be inferred; rather, the company must obtain the consumer's intent.

To be most effective, the Commission suggests that choices should be clearly and concisely described and offered when – and in a context in which – the consumer is making a decision about his or her data. Depending on the business model, this may entail a "just-in-time" approach, whereby a company presents the choice to the consumer at the point at which he or she enters personal data (such as in an online retail transaction) or accepts a product or service (such as at checkout in an offline transaction).

Other than to say that stricter requirements should apply to the collection of sensitive data and the collection of personal data from sensitive populations (such as children), the Commission has declined to specify whether or when opt-in versus opt-out consent must be obtained. It has requested comment on this and other issues – including what should be considered sensitive information – so the final framework may provide guidance on these issues.

We expect that this portion of the Commission's preliminary report is the most likely aspect of the report to result in enforcement actions in the near term. Requiring clear notice and choice for non-obvious aspects of a company's data collection practices has its roots in FTC spyware cases in the early 2000s. The Commission has maintained this position since then, most recently enforcing it in the context of alleged data transfers to third parties disclosed deep within a company's End User License Agreement.[3]

- **Support for Do Not Track.** The Commission has taken the position that the most "practical" way to offer consumers a choice in the context of online behavioral advertising is via a universal do not track mechanism. This would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser, signaling his or her choices about being tracked online. The Commission seeks comments on a variety of issues related to this proposal, including whether any such mechanism should offer consumers granular options (e.g., to control the types of advertising they receive or the types of data collected about them).

[3] See Federal Trade Commission v. EchoMetrix, Inc., CV10-5516 (E.D.N.Y., November 30, 2010).

The Commission is careful to note that it does not believe that it has the legal authority to develop and implement a do not track requirement and suggests that it must be done by either the private sector or through legislation. Already, some members of Congress have suggested that they support some form of do not track legislation. It is not clear whether such legislation will move in the 111th Congress. Nor is it clear that a broad-based, industry-developed do not track program will emerge any time soon. Rather, we expect that individual companies will compete to offer their own, private do not track programs and seek to build large audiences of subscribers among web publishers and advertisers who may feel an incentive to subscribe to protect their brands. These efforts could consolidate, they could exist side-by-side in the market, or, eventually, one may emerge as a market leader. In any event, it is not unlikely that the market will work to address this Commission concern, driven by the incentive that brands continue to feel to be privacy friendly.

3. GREATER TRANSPARENCY

The framework proposes a variety of measures aimed at improving the transparency of companies' data practices for consumers. Specifically, companies should:

- **Make their privacy policies clearer, shorter and standardized, so that a consumer can understand them more easily and be able to compare them across companies.** At this time, the Commission has not proposed any particular standardized format, although it has noted work on standardized notices in the Gramm-Leach-Bliley Act context as a possible guidepost. Nor has the Commission made clear that it intends to enforce Section 5 against companies for failure to standardize their privacy policies, or even to make them clearer.
- **Provide consumers with reasonable access – based on the costs and benefits of access in a particular situation – to the data companies hold about them.** This applies even to companies that do not interact directly with consumers, such as data brokers. The Commission has asked for comment on the feasibility of this, but it is clearly something they want to encourage, if not one day mandate.
- **Provide robust notice and obtain express consent before using consumer data in a materially different way than claimed when the data was collected.** This proposal is consistent with the Commission's enforcement activity and prior industry guidance.[4]
- **Work with other stakeholders to educate consumers about commercial data practices.**

CONCLUSION

Overall, the report makes clear the Commission's 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 the Commission goes in turning this fundamental concern into enforceable requirements will depend on the comments it receives and the support it gets from Congress.

Contact:

Reed Freeman
(202) 887-6948
rfreeman@mofo.com

Julie O'Neill
(202) 887-8764
joneill@mofo.com

[4] *See, e.g.*, *Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004); OBA Report, note 37.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.