FTC Releases Proposed Framework for Protecting Consumer Privacy

Dana B. Rosenfeld

December 8, 2010

Introduction

Last week, the Federal Trade Commission ("FTC") issued its highly-anticipated preliminary staff report on privacy, "*Protecting Consumer Privacy in an Era of Rapid Change*." The report follows a series of three public roundtables on the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer data.[1] The report proposes a new privacy framework for businesses and policymakers and addresses the FTC staff's view that self-regulation has, up to now, failed to provide adequate consumer protection. The proposed framework is intended to be implemented by commercial entities, regardless of whether such entities interact directly with consumers, and would apply to the online and offline data handling practices of consumer data that can be reasonably linked to a specific consumer, computer, or device.

Rationale For the Proposed Framework

The proposed framework builds upon the harm-based and notice-and-choice models that the FTC has used to protect consumers' personal information in the marketplace. Due to shifting industry practices and technological changes, the FTC staff believes that current models provide increasingly limited protection for consumers. For example, the staff report notes that current privacy policies have become increasingly complex and more focused on limiting corporate liability, which they believe has made it more difficult for consumers to make informed decisions. The report also notes that greater computing power allows companies to combine personally identifiable information ("PII") with non-personally identifiable information in a manner that blurs the distinction between PII and non-PII information.

The FTC staff anticipates that the proposed framework will allow it to respond more effectively to practices of concern and reduce consumer misunderstanding about the collection and use of personal data, and consumers' corresponding inability to make informed choices (in the staff's view).

The Commission will continue to use its authority under Section 5 of the FTC Act, and other statutes it enforces, to investigate and enforce privacy or data security practices that may violate such laws.

Recommendations Within the Proposed Framework

The proposed framework includes three primary recommendations: (1) privacy by design; (2) simplified choice for consumers on how their data is handled; and (3) greater transparency for consumers on privacy practices. These recommendations are described in detail below.

Privacy By Design

The FTC staff proposes that companies incorporate consumer privacy protections into their everyday business processes and at each stage of product or service design and development. Under this approach, companies should employ reasonable safeguards for the collection, retention, and disposal of consumer data. The level of required security would depend on the sensitivity of the data and the nature of the company's business.

Data Collection, Retention and Disposal: The collection of customer information should be limited to areas where there is a legitimate business need. For example, a company that collects customer information only to later aggregate the data and sell it to a third-party would fall outside the FTC staff's proposed view of legitimate practices. Further, the collected information should be retained only for a reasonable period of time, which the report defines as the period for which the legitimate reason for collecting the information endures. The report highlights location-based data as one example of information that companies should not retain longer than necessary. Finally, once the legitimate use has ended, companies must securely dispose of the data.

Data Accuracy: The FTC staff proposes that companies take reasonable steps to ensure the accuracy of consumer data within their possession so that consumers are not denied benefits or suffer harm due to erroneous information.

Privacy Procedures and Personnel: The report proposes that companies maintain comprehensive data management procedures throughout the life cycle of their products and services, and include privacy reviews at the outset of product research and development. Further, companies should assign dedicated personnel to oversee privacy issues, train employees on privacy practices, and promote accountability for privacy policies throughout the organization.

Simplified Choice

The staff report proposes that companies segment their consumer data practices into those that are "commonly accepted" and those that are "not commonly accepted," which will in turn inform companies on the proper controls to impose on the collected information. Although the report provides examples of "commonly accepted" and "not commonly accepted" practices, it seeks public comment on whether these lists are too broad or too narrow.

Commonly Accepted Practices: Companies using commonly accepted practices would not be required to seek prior consent once the consumer elects to use the product or service. Examples of commonly-accepted practices include:

1. Product and service fulfillment
2. Internal operations
3. Fraud prevention
4. Legal compliance and public purpose
5. First-party marketing (*e.g.*, product recommendations based on prior purchases)
6. Contextual advertising

Not Commonly Accepted Practices: Companies that use practices that are, in the staff's view, not commonly accepted would be required to give consumers the ability to make informed and meaningful choices based on consent through means that are easy for the consumer to locate and

understand. For example, choices identified deep within a lengthy privacy policy and pre-checked boxes would be, in the staff's view, an ineffective means of obtaining meaningful consent under the proposed framework. Practices considered not commonly accepted include:

1. Deep packet inspection for the purpose of creating marketing profiles on consumers
2. The sale of data to a data broker or other third-party unknown to the consumer
3. Online behavioral advertising

Do Not Track: The FTC staff supports a "Do Not Track" tool that would let consumers decide whether to receive or opt-out from targeted ads based on practices such as online behavioral advertising. The FTC report acknowledges that online behavioral advertisements fund online content and provide personalization of advertisements, and indicates that any solution should not undermine these benefits. Nevertheless, FTC staff believes that industry efforts have fallen short. Since 2008, the FTC has pushed, and continues to push, for a "just in time" mechanism to provide consumers with information and choices about behavioral advertising. Despite recent industry developments, there is not yet an industry-wide solution available to consumers, and staff do not believe that consumers are aware of, or understand, current privacy tools. The FTC, during a question and answer session hosted on Twitter, expressed its desire that companies act quickly on the Do Not Track feature.

The day after the FTC staff released its report, the Commerce, Trade, and Consumer Protection Subcommittee of the House Committee on Energy and Commerce held a hearing on the feasibility of Do Not Track legislation. Technology experts stated that it would not be technically feasible to regulate IP addresses in the same way as telephone numbers and such a Do Not Track mechanism would disrupt a user's online experience. FTC Director of the Bureau of Consumer Protection David Vladeck disputed that view, stating that a Do Not Track registry is "technically feasible."

The report proposes a browser setting, similar to a persistent cookie, that conveys information to sites visited by consumers using that browser to signal whether the consumer wants to be tracked or receive targeted ads. The FTC staff advocates the browser-based model because, unlike the Do Not Call registry that captures individual telephone numbers, there is no equivalent persistent identifier for computers as IP addresses often change.

The FTC staff suggests in the report that a Do Not Track mechanism could be accomplished by legislation or robust, enforceable self-regulation. Although legislators have released multiple privacy and data security bills for discussion[2], Representative Markey (D-MA) announced at the House Subcommittee hearing that he plans to propose legislation next term that would impose Do Not Track requirements on companies prohibiting targeted marketing to children. Such legislation could be seen as a first step toward more comprehensive online behavioral marketing laws. Vladeck further stated at the House Subcommittee hearing that if Congress chooses to enact legislation, the Commission will seek authority to conduct rulemaking and to obtain civil penalties to enforce the legislation.[3]

Increased Transparency

The report proposes increased transparency to provide choice mechanisms in a prominent, relevant and easily accessible place for consumers.

Privacy Policies: Privacy policies should be clear, concise and brief to the extent possible, so that

consumers can more clearly determine who is collecting consumer data, why it's being collected, and how the data will be used. Further, FTC staff recommends some level of standardization among policies so that consumers can compare privacy policies across companies, with the effect of driving industry competition based on privacy practices.

Consumer Access to Data: The report proposes that companies should provide reasonable access to the consumer data they maintain. The Commission staff supports a sliding-scale approach, whereby the extent of access would depend on the sensitivity of the data and its intended use.

Prominent Disclosures: Consistent with existing FTC policy and previous enforcement actions, under the proposed framework, the report suggests that companies provide prominent disclosures and obtain affirmative express consent before using the data in a materially different manner than claimed when the data was collected, or when making retroactive changes to data policies. For example, if a social networking site changes its policy of keeping profile information private, it should make a prominent disclosure and seek affirmative express consent before retroactively applying the new policy.

Education: The FTC staff proposes that companies encourage and participate in greater consumer education to increase awareness and understanding of commercial data privacy practices and their privacy implications for consumers.

Conclusion

The proposals within the preliminary report are not directly enforceable regulations, but they are instructive and provide insight on what businesses can expect in privacy enforcement trends in the future. As a result, companies should consider these recommendations as they review or modify existing information collection, use, and data retention policies and practices, and when entering into new agreements with service providers. While it may not be possible to predict with certainty the precise outcome of the staff recommendations, it is clear that the FTC is poised to change or at least shift longstanding principles of notice and choice and address widespread consumer concerns regarding behavioral advertising.

The FTC staff encourages comments on all issues raised within the report concerning the proposed framework and it invites responses to specific questions contained in Appendix A of the report. The filing deadline for comments is January 31, 2011. Please contact us, if we can be of assistance in the preparation of comments on your behalf.

Kelley Drye will be hosting a complimentary Privacy Seminar to discuss the FTC's Privacy Report, as well as other topic issues, on January 20. Stay tuned for further details. We also note that the ABA Privacy & Information Security Committee (within the Section of Antitrust) is holding a complimentary audio program, *The FTC's New Privacy Report: What You Need to Know*, on December 14, 2010. More information on the ABA program can be found here.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements

with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this advisory, contact:

Dana B. Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

---

[1] Information about the FTC's privacy roundtables can be found in Kelley Drye & Warren's March 29, 2010, February 3, 2010, and December 15, 2009 client advisories.

[2] *See, e.g., Representative Boucher Introduces Privacy Legislation*, Kelley Drye & Warren Client Advisory (May 5, 2010), *available* here.

[3] *Hearing on "Do Not Track Legislation: Is Now the Right Time?" Before the Subcomm. On Commerce, Trade, and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. 2 (2010) (statement of David Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission) at 18, *available at https://democrats-energycommerce.house.gov/*.