Federal Trade Commission Releases Proposal for Consumer Privacy Protection: How Would the Commission's Proposed New Framework Alter Business Practices, Particularly Online?

In a preliminary report designed to "guide and motivate industry,"[1] the Federal Trade Commission (FTC or Commission) has proposed a new framework for addressing privacy concerns in connection with the commercial use of consumer data. The preliminary report (the Privacy Report) is sweeping in scope and highly ambitious with respect to providing consumers with meaningful choice about the collection and use of their data, and increasing the transparency of such collection and use. If the FTC adopts the principles set forth in the Privacy Report, whether by incorporating them in regulations or guidance, pressing Congress to enact them in legislation, or simply applying them through enforcement proceedings, many businesses will need to take a variety of steps to limit their collection, use, and disclosure of consumer information beyond what current law requires.

Businesses that rely on consumer data for analytical, transactional, marketing, and any of a host of other purposes need to consider *now* whether and how the FTC's proposed approach will affect them. The Commission has invited comments on the Privacy Report, which are due on or before **January 31, 2011.** The Commission plans to issue a final report later in 2011.

Background

Until now, the FTC's protection of consumer privacy has taken two forms: the notice-and-choice model and the harm-based model. The notice-and-choice model was the earliest put forward by the FTC and encouraged companies to develop privacy notices describing their data collection practices. This ensured that consumers could make informed choices, determining whether or not to disclose personal information to a company based on what the privacy policy promised or did not promise. The harm-based model consisted of enforcement actions, under the FTC's statutory power, to address alleged failures in the protection of consumers' personal information–including companies' alleged non-

1 *Protecting Consumer Privacy in an Era of Rapid Change—A Proposed Framework for Businesses and Policymakers,* Preliminary FTC Staff Report (hereafter, the "Privacy Report"), December 2010, p. 2.

Contacts

Nancy L. Perkins
+1 202.942.5065

Amy Ralph Mudge
+1 202.942.5485

Ronald D. Lee
+1 202.942.5380

Stephanie M. Phillipps
+1 202.942.5505

compliance with their own privacy policies. According to the FTC, notice-and-choice has had limited success, because consumers do not read lengthy privacy policies, and harm-based enforcement is an inefficient and incomplete method of protecting privacy.

Recognizing consumers' interest in protecting their privacy and the need to reduce the burden on consumers to do so, the FTC seeks to expand the scope of consumer data privacy regulation to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device,"[2] including companies that are not consumer-facing. However, the FTC has solicited comments on this proposed scope, including those with respect to the following questions:

- Should certain types of businesses be excluded from the framework?
- Is it feasible for the framework to apply to all data that can be reasonably linked to a specific consumer, computer, or other device? What about data that may become linkable in the future? Are there any alternatives?
- Are there technical measures that could "anonymize" data?

Core Aspects of the Proposed Framework

The FTC's proposed framework is structured around three broad principles, with specific suggestions for the implementation of each one: (1) privacy by design, (2) consumer choice, and (3) transparency. For each aspect of the proposed framework, the FTC has requested comments.

Privacy by Design. "[C]ompanies should incorporate substantive privacy and security protections into their everyday business practices and consider privacy issues systemically, at all stages of the design and development of their products and services."[3] The Privacy Report proposes that companies build certain privacy protections into their everyday operations in four specific ways:

a. *Companies should reasonably protect data.* Companies should reasonably protect data, with the level of protection appropriate to the sensitivity of the information and the risks a company faces from inadvertent disclosure. The Privacy Report notes that a number of Federal and State laws already require this level of protection, and the FTC already takes regular enforcement action in pursuit of this standard. However, the FTC has solicited comments on how to determine the 'sensitivity' level of information.

b. *Companies should only maintain needed information.* Companies should only collect information required to fulfill a specific and legitimate business need. For example, if an advertising network is tracking online activities merely to serve targeted ads, there is no reason to use key loggers. If a mobile application is providing weather updates, there is no need for the application to collect contact lists or call logs. But who is to determine what is a "specific and legitimate business need" in contexts not explicitly addressed by the FTC? Could the FTC create a definition that that would provide sufficient guidance to businesses on the definition of such need? The Privacy Report solicits comments on whether and how the concept of "specific business purpose" or "need" should be further defined.

c. *Reasonable and appropriate data retention periods.* Companies should retain information only as long as the specific, legitimate business need exists. Location-based data collected from mobile devices, for example, if collected and stored over time, can reveal personal information about an individual (such as repeated visits to a particular location over a particular period of time) that may not be needed by the data collector, but if accessed by others could risk harm to the individual. The FTC has solicited comments on how to determine a reasonable retention period.

d. *Ensuring the accuracy of data.* Companies should ensure the accuracy of the data they collect, particularly if the data is potentially harmful or may result in the denial of certain benefits. Incorrect identity-verification information, for example, can prevent consumer access to their bank accounts or services.

2 Privacy Report, p. 42.

3 Privacy Report, p. 44.

The Privacy Report proposes that companies incorporate data management procedures into the life cycle of their products and services. Such procedures should include the designation of specific personnel responsible for oversight of privacy policies. Companies should also use privacy-enhancing technologies, such as identity management, data tagging tools and encryption. One question raised by the FTC, in this context, is whether companies can minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests.

Consumer Choice. The proposed framework requires companies to provide consumers with meaningful choice, but sets forth a limited set of data practices for which choice is not necessary.

a. *Consumers should be able to make informed and meaningful choices.* For the collection of most commercial data, consumers should be given a choice about the release of information, and that choice should be available at the time of the information entry. With respect to online retailers, for example, "the disclosure and control mechanism should appear clearly and conspicuously on the page on which the consumer types in his or her personal information."[4] These requirements would govern mobile communications as well, and would apply to carriers, operating system vendors, applications, and advertisers. The proposal would also require consumer choices to be "durable," and not subject to repeated requests from the same merchant. The FTC has solicited comments on a number of questions related to consumer choice, for example:

   - What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category? Should the method of consent be different for different contexts?
   - Is a standardized-consent mechanism feasible?
   - Are "take it or leave it" propositions appropriate?

b. *Commonly accepted practices.* Certain "commonly accepted practices" would not require consent. These practices include product and service fulfillment, such as the collection of an address for product shipment. Certain internal operations are also commonly accepted practices, such as collection of information about visits and click-through rates to improve site navigation. Other commonly accepted practices include fraud prevention, legal compliance, and first-party marketing, (e.g., recommending a product based on consumers' prior purchases on the same website). However, an online publisher's allowing of a third party to collect data about consumers' use of the website, as part of online behavioral advertising would not be "commonly accepted." Also unacceptable would be tracking online activities by an Internet Service Provider (ISP) through "deep packet inspection"–i.e., inspecting the content of email and website visits.

   It is not at all clear that there is a uniformly understood body of practices recognized to be "commonly accepted." The FTC has specifically invited input to help define "commonly accepted practices," asking:

   - Is the list of proposed "commonly accepted practices" too broad or too narrow? Are there practices that should be considered "commonly accepted" in some business contexts but not in others?
   - Should first-party marketing be limited to the context in which the data is collected from the consumer? Should marketing to consumers by commonly branded affiliates be considered first-party marketing?
   - Should a company be able to "enhance" its data by obtaining customer information from other sources?

c. *Do not track.* The framework proposes that consumers be given the ability to opt out of the tracking of their online browsing. The mechanism would have to be a browser-based method of conveying to sites that the consumer does not want to be tracked or receive targeted advertisements. Recognizing the technical challenges, the FTC has asked the industry to comment on how such a mechanism could be offered, and in

4 Privacy Report, p. 58.

particular, whether such an opt-out scheme should be extended to mobile applications.

Transparency. The proposed framework requires companies to increase the transparency of their data practices. Company data policies should be easily accessible, and companies should notify consumers before making changes to these policies. Furthermore, consumers should be given reasonable access to their data and be educated about commercial data practices.

a. *Privacy notices should be shorter, clearer, and more standardized.* Although most companies now disclose their data practices through privacy notices, some bury disclosures of important information. Privacy notices, in the mobile context, pose particular difficulties because the small screens of mobile devices mean that a privacy notice can be spread over as many as 100 separate screens. The proposed framework requires privacy notices to clearly and concisely articulate who is collecting data, why they are collecting it, and how such data will be used. Companies must also prominently disclose when they use information differently than first claimed, and obtain affirmative consent to do so.

b. *Companies should provide reasonable access to consumer data.* The combination of information from various sources by information brokers can result in the creation of individual consumer profiles, over which the consumer has no control. If appropriate—such as for identity authentication or decision-making purposes—the ability of the consumer to delete certain data should be considered.

   The FTC posed a number of questions related to transparency issues:

   - Is the standardization of privacy terminology feasible?
   - How can companies present these notices effectively on mobile and similar devices?
   - Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?
   - Is it feasible for the industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

Possible Related Legislation

In response to the FTC Privacy Report, there are already moves to step up legislative action, with respect to Internet privacy. After the release of the report, Senator John Kerry (D-Mass.), Chair of the Senate Commerce Committee's Subcommittee on Communications, Technology, and the Internet, announced that he plans to introduce online consumer privacy protection legislation early in 2011, stating that the Privacy Report provides an important confirmation of conclusions he has reached in considering privacy legislation.

Reportedly, the legislation Kerry plans to introduce would include a "Safe Harbor" mechanism available to firms that comply with FTC data privacy and security "best practices." Under the legislation, the FTC would have the authority to approve Safe Harbor status for particular firms (presumably in a manner similar to that currently used by the Department of Commerce under the Safe Harbor mechanism, agreed to by the United States and the European Union, with respect to transfers of personal information from the EU member nations to the United States). Entities granted Safe Harbor status would be subject to FTC oversight and penalties, but would not be subject to private lawsuits or complaints filed with the FTC.

Possibly, the bill planned by Senator Kerry will incorporate some elements of the bill already introduced by Representative Bobby L. Rush (D-Ill.) in July 2010 (H.R. 5777), which, in addition to establishing data privacy and security standards, would similarly create a Safe Harbor mechanism for companies that adhere to those standards and participate in one or more industry self-regulatory programs approved by the FTC.

Republican Members of Congress also responded quickly to the release of the FTC Privacy Report, including Representative Joe Barton (R-Tex.), the Ranking Member of the House Energy and Commerce Committee, who pledged to explore the value of Internet privacy policies

and how to make them more meaningful and effective; and Representative Cliff Stearns (R-Fla.), who said he plans to work further on online data privacy legislation in the coming year.

The FTC's solicitation of comments on the framework proposed in the Privacy Report offers an opportunity for affected parties to participate in the development and potentially influence the outcome of the final framework adopted by the Commission. If you have questions about the Privacy Report or are interested in submitting comments, please contact any of the attorneys named below or your principal contact within Arnold & Porter LLP.

Nancy Perkins
+1 202.942.5065
Nancy.Perkins@aporter.com

Amy Ralph Mudge
+1 202.942.5485
Amy.Mudge@aporter.com

Ronald D. Lee
+1 202.942.5380
Ronald.Lee@aporter.com

Stephanie M. Phillipps
+1 202.942.5505
Stephanie.Phillipps@ aporter.com

Michael Levin
+1 212.715.1025
Michael.Levin@aporter.com