

# FTC Goes Public with Staff Preliminary Report on Online Privacy Issues

## Prepared By:

David Jacoby and Judith S. Roth  
of the Data Privacy Client Service Team

## What Happened

The staff of the Federal Trade Commission (“FTC” or “Commission”) issued a long-awaited preliminary report (the “Report”) on consumer privacy in December, another step on the road to the issuance of FTC guidelines in this complex area. The 122-page Report (“Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers”) proposes safeguards for data gathered about consumers, both on- and offline. The most controversial proposal is the creation of a “Do Not Track” concept that would let consumers opt out of collection and sale of their browsing and other data gleaned online.

The framework is only conceptual, with many practical aspects unaddressed. Public comment on the Report’s proposals and its real-world application is sought through the end of January, 2011.

The three principal areas addressed in the Report are:

1. **Privacy by Design** Companies should adopt a “privacy by design” approach, building consumer data protections and considerations into every stage of all business practices. This would include management of consumer data throughout the life cycle of products and services provided.
2. **Simplified Privacy Choice** Consumers should be given simple, easy-to-understand choices about the use of their data. The FTC staff discusses standardized ways to accomplish that, which could include examples such as standardized formats for choices and creating notices alerting consumers to choices that they would see just before submitting data. In the sensitive area of behavioral advertising, the FTC staff’s preferred solution would be a browser-implemented “Do Not Track” button, akin to the “Do Not Call” registry for telemarketers. Some commonly accepted practices, such as getting a shipping address for delivery purposes, would not require consent.
3. **Greater Transparency** Data policies should be more transparent and more available to consumers. This requirement would apply even to entities that do not

deal directly with consumers, such as data brokers. Upon request, companies should have to provide reasonable access to consumer data they maintain. Companies should obtain express consumer consent to any use of data that differs materially from the original use. Additionally, broad efforts to educate consumers about commercial data gathering and available choices should take place.

## **What's Changed**

Some of the concepts embodied in the framework have been FTC objectives for many years, including affording consumers notice of, and choice as to, uses of their private information; allowing access to data collected; and requiring protection for the collected information.

The Report recognizes, however, that technological change has upset what used to be clear boundaries. Just as electronically stored information has altered profoundly discovery in litigation, the abundance of data and the increasing technical ability to manipulate it has transformed how businesses can match up and use data. Appropriately, the FTC recently hired its first "technologist" to help assess these issues.

Once upon a time, it was thought sufficient to control disclosure of "personally identifiable information," such as names and Social Security numbers. Now, however, increasing data capture, storage and analytical capacity allows pinpoint identification of nominally anonymous consumers. It also allows the identification of individual devices through which online access is obtained. As a result, businesses can transmit messages to highly targeted groups even without knowing an actual individual's identity. The consumer data which permits such targeting is highly prized. It fetches top dollar from advertisers and pays the freight for various free services, like browsers.

Technology also has provided the ability to link the data about browsing or even about an individual consumer's computer back to a specific individual through correlation of other data. For example: if one knows that a given mobile device with a geolocation feature is always at a given location once a week, and that the location is a cancer treatment center, there is disclosure of highly sensitive information about the device's owner. If one then correlates that data with data generated by the device user's participation in a social network, one may be able to conclude a specific individual is undergoing cancer treatment.

The Report recognizes that earlier insistence on privacy policy disclosure, including by the FTC, has created a monster of sorts: prolix, pages-long company privacy policies written in legalese, which few people — including, as the Report notes, even the Chief Justice of the United States Supreme Court — bother to read. Nevertheless, the staff continues to hope that clearer, simpler privacy choices will promote competition on the basis of privacy policies.

### **What It Means**

The Report tackles an enormously complex issue, which seems to morph almost from month to month. Yet the Report itself is not final, much less constituting a set of final FTC Guidelines. It has been almost three years since the first FTC roundtable to discuss these issues.

The FTC staff spends almost a quarter of the Report detailing the FTC's history of involvement with privacy issues. One can read that history in a variety of ways, but it was no doubt intended in part to try to assert the Commission's primacy in the field. As the report appeared, Congressional hearings were going on, draft legislation had been circulated on Capitol Hill, and the White House was reviewing a Commerce Department draft, since released, which addressed many of the same subjects and calls for a federal privacy policy office, so jurisdictional issues also may be on the horizon.

We recommend that businesses affected by the proposed framework consider offering comments on the Report. Much of what the staff seeks to learn are the real-world applications of the general concepts the report discusses. And if you happen to have a Do Not Track button ready for installation on browsers, we know someone who'd like to hear about it.

© 2011 Schiff Hardin LLP

This publication has been prepared for the general information of clients and friends of the firm. It is not intended to provide legal advice with respect to any specific matter. Under rules applicable to the professional conduct of attorneys in various jurisdictions, it may be considered advertising material.

For more information visit our Web site at [www.schiffhardin.com](http://www.schiffhardin.com).