



January 2011

**PRIVACY & INFORMATION
SECURITY UPDATE****FTC Issues Long-Awaited Privacy Report**

In December 2010 the Federal Trade Commission (FTC) issued an extensive report on consumer privacy following a series of roundtable discussions it conducted in 2009. Key points of the report, “Protecting Consumer Privacy in an Era of Rapid Change: Preliminary FTC Staff Report” (“Report”), are summarized below. Privacy issues are likely to remain at the top of legislative and regulatory initiatives over the next year.

FRAMEWORK FOR PROTECTION

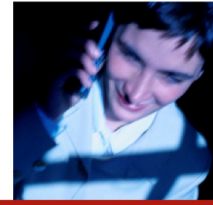
The Report begins with the presumptions that many businesses do not adequately address consumer privacy interests and that industry must “do better.” The Report sets forth a framework for how companies should protect consumers’ privacy. The proposed framework would apply broadly to *online and offline* commercial entities that collect, maintain, share or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device (*i.e.*, the framework is not limited to those that collect personally identifiable information, or PII). This broad scope is intended to reach entities that collect data including those such as data brokers that generally do not interact directly with consumers. The FTC initially requested comments on the Report by January 31, 2011, but just extended the deadline to **February 18**. After reviewing the comments received, the FTC will issue a final report later in the year.

In the interim, the FTC states that it will continue to enforce its laws in the privacy area, using its existing authority under Section 5 of the Federal Trade Commission Act and other consumer privacy laws (*e.g.*, Gramm-Leach-Bliley Act, Children’s Online Privacy Protection Act, CAN-SPAM Act and the Telemarketing and Consumer Fraud and Abuse Prevention Act). Once the framework is finalized, FTC staff may conduct surveys or use other benchmarks to evaluate the extent to which industry is implementing the concepts in the framework.

The three main components of the Report’s privacy framework are:

Building a “privacy by design” approach by building privacy protections into companies’ everyday business practices.

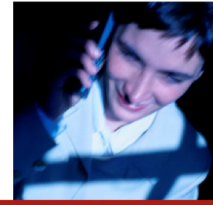
- These protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used and implementing reasonable procedures to promote data accuracy.



- The Report further encourages companies to implement and encourage procedurally sound privacy practices throughout their organizations, *e.g.*, assigning personnel to oversee privacy issues, training employees on privacy issues and conducting privacy reviews when developing new products and services.
- Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.
- Safeguards should include physical, technical and administrative safeguards to protect information.

Providing choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past.

- Under this approach, consumer choice would *not* be necessary for a limited set of “commonly accepted” data practices. The Report states that it is reasonable for companies to engage in certain commonly accepted practices – *e.g.*, product and service fulfillment, internal operations to improve services offered, fraud prevention, legal compliance and first-party marketing (though companies should still disclose these practices in their privacy policies to promote transparency).
- Online contextual advertising where advertisements are delivered based on a consumer’s current visit to a web page or single search query, without the collection and retention of data about the consumer’s online activities over time, should fall within the “commonly accepted practices” category.
- For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.
- The most practical method of providing universal choice in the case of behavioral advertising would likely involve the placement of a persistent setting (similar to a cookie) on the consumer’s browser signaling the consumer’s choices about being tracked and receiving targeted ads (“Do Not Track”).
- Where the consumer elects not to have information collected, used or shared, that decision should be durable and not subject to repeated additional requests from the particular merchant.
- Choices buried within long privacy policies and pre-checked boxes are not effective means of obtaining meaningful, informed consent.
- Certain types of sensitive information warrant special protection, such as information about children, financial and medical information, and precise geolocation data.



Making data practices more transparent to consumers.

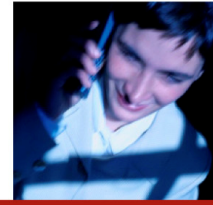
- Clearer, concise and easy-to-read privacy policies may play an important role here.
- FTC staff also proposes providing consumers with reasonable access to the data that companies maintain about them, particularly companies such as data brokers who do not interact with consumers directly.
- Extent of access should be proportional to the sensitivity of the data and its intended use.
- All entities must provide robust notice and obtain affirmative consent for material, retroactive changes to data policies.
- A broad effort should be undertaken to educate consumers about commercial data practices and the choices available to them.

DO NOT TRACK

The FTC staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, called “Do Not Track.” This mechanism could be accomplished by legislation or possibly by robust, enforceable self-regulation. The FTC believes that the most practical method would involve placing a setting similar to a persistent cookie on a consumer’s browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. There must be an enforceable requirement that sites honor those choices in order for this method to be effective.

ISSUES FOR COMMENT

The Report seeks comment on several different issues, including whether certain types of companies or businesses should be excluded from the framework (*e.g.*, businesses that collect, maintain or use a limited amount of non-sensitive consumer data). The FTC also seeks input on what technical measures exist to more effectively “anonymize” data. Other topics include whether there are additional substantive protections that companies should provide and how to balance the costs and benefits of such protections; whether the proposed list of “commonly accepted practices” is too broad or narrow; how the proposed framework should handle the practice of data “enhancement,” whereby a company obtains data about its customers from other sources – offline and online – to enrich its databases, and whether companies should provide choices about this practice; what methods of consent should be used; and what types of choice mechanisms should be employed for data brokers including whether some sort of universal, standardized mechanism would be feasible and beneficial. The Report and the full list of issues for comment are available at www.ftc.gov/os/2010/12/101201privacyreport.pdf.



FOR MORE INFORMATION

For more information, please contact:

Michelle W. Cohen	202.263.4151	Michelle.Cohen@ThompsonHine.com
Thomas F. Zych	216.566.5605	Tom.Zych@ThompsonHine.com
Joanne E. Clifford	216.566.5758	Jodi.Clifford@ThompsonHine.com

If you do not wish to receive future communications by email, please send an email with “unsubscribe” in the subject line to **Unsubscribe@ThompsonHine.com**.

This advisory may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions. Some of the design images and photographs in this document may be of actors depicting fictional scenes.

© 2011 THOMPSON HINE LLP. ALL RIGHTS RESERVED.