LOEB & LOEB LLP

Advanced Media and Technology Law

ALERT

MARCH 2012

Privacy Law

FTC Releases Final Version of Privacy Report

The Federal Trade Commission has released the final version of its Privacy Report titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers."

The FTC issued a Preliminary Privacy Report in December 2010 which proposed a new privacy "framework" for protecting consumer privacy and called on industry to improve self-regulatory efforts. Since the December 2010 Report, the FTC announced several important enforcement actions, proposed changes to the Children's Online Privacy Protection Rule, conducted a survey of mobile apps directed to children, held several public workshops, and requested public comments in response to the Preliminary Report.

The Final Privacy Report has several components:

i. The privacy framework, which has been modified slightly, is intended to serve as "best practices" for companies that collect and use consumer data.

ii. Recommendations for new federal legislation in three key areas: (1) legislation providing baseline consumer privacy protections, (2) the regulation of data brokers, and (3) security breach notification.

iii. Recommendations for improvements to self-regulatory programs.

1. Privacy Framework

The FTC's privacy framework is consistent with the Fair Information Practice Principles first articulated almost 40 years ago and is intended as "best practices" for businesses that collect and use consumer data:

- **Privacy by Design:** Build in privacy at every stage of product development;
- **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- **Greater Transparency:** Make information collection and use practices transparent.

In the Final Report, the Commission made some changes to the framework's scope. The Preliminary Report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. The FTC also clarified that data is not "reasonably linked" to consumers if a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data. The FTC reiterated that the framework applies to online and offline data.

The Commission also revised its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the Preliminary Report set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). In the Final Report, the Commission is proposing a modified approach that focuses on the context of the consumer's

interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the Preliminary Report would generally meet this standard, there may be exceptions.

2. Recommendations for New Federal Legislation

The Commission recommends that Congress consider enacting targeted legislation to increase transparency and provide consumers with more control over the practices of information brokers. The FTC noted that consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data. Such legislation could provide consumers with reasonable access to data that such companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. In addition to federal legislation, the FTC is calling on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

The Commission is also calling on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate. The FTC suggested that such legislation will complement the privacy approach articulated by the Consumer Privacy Bill of Rights that was proposed by the White House in February. (We provided a summary of the White House proposal in a previous Alert.)

3. Self-Regulatory Programs

The FTC urges industry to accelerate the pace of self-regulatory measures to implement the Commission's final privacy framework. The FTC identified the following major action items:

- **Do Not Track:** While recognizing that browser vendors have developed tools that consumers can use to signal that they do not want to be tracked and the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools, the FTC stated that "the work is not done" and the Commission will work with these groups "to complete implementation of an easy-to use, persistent, and effective Do Not Track system."

Specifically, the FTC proposes that any Do Not Track system should include five key principles. First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (e.g., preventing click-fraud or collecting de-identified data for analytics purposes).

- **Mobile:** The Commission is urging companies that provide mobile services to improve privacy protections, including the development of short, meaningful disclosures that address data collection, transfer, use, and disposal, particularly for location data. The FTC will host a workshop on May 30, 2012, and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

- **Enforceable Self-Regulatory Codes:** The Consumer Privacy Bill of Rights proposed by the White House will be the basis for a voluntary set of sector-specific codes of conduct. The FTC will work with the Department of Commerce to develop these codes of conduct. The FTC stated that it will view a company's compliance with those codes of conduct favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

For more information about these developments, or any other privacy concerns, please contact Ieuan Jolly at ijolly@loeb.com or 212.407.4810.

If you received this alert from someone else and would like to be added to the distribution list, please send an email to alerts@loeb.com and we will be happy to include you in the distribution of future reports.

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

Circular 230 Disclosure: To ensure compliance with Treasury Department rules governing tax practice, we inform you that any advice contained herein (including any attachments) (1) was not written and is not intended to be used, and cannot be used, for the purpose of avoiding any federal tax penalty that may be imposed on the taxpayer; and (2) may not be used in connection with promoting, marketing or recommending to another person any transaction or matter addressed herein.

Advanced Media and Technology Group

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ROBERT M. ANDALMAN	RANDALMAN@LOEB.COM	312.464.3168
ALISA C. BERGSTEIN	ABERGSTEIN@LOEB.COM	312.464.3155
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
NATASHA CHAMILAKIS	NCHAMILAKIS@LOEB.COM	212.407.4853
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
THOMAS A. GUIDA	TGUIDA@LOEB.COM	212.407.4011
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE HOWARD	MHOWARD@LOEB.COM	310.282.2143
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
MICHAEL RIDGWAY JONES	MJONES@LOEB.COM	212.407.4042
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DOUGLAS E. MIRELL	DMIRELL@LOEB.COM	310.282.2151
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
DANIEL O'CONNELL OFFNER	DOFFNER@LOEB.COM	310.282.2252
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON POLLOCK SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
STEVE A. SEMERDJIAN	SSEMERDJIAN@LOEB.COM	212.407.4218
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
REGAN A. SMITH	RASMITH@LOEB.COM	312.464.3137
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960