Doing Business in the Age of Enforcement: Key Areas of FTC and FCC Scrutiny in Advertising, Privacy and Targeting

Wednesday, May 11, 2011

Kenneth Florin
Partner and Co-Chair, Advanced Media and Technology Department;
Chair, Emerging Media Practice Group
kflorin@loeb.com | 212.407.4966

Walter Steimel, Jr.
Partner, Advanced Media and Technology Department
wsteimel@loeb.com | 202.618.5015

LOEB & LOEB LLP

Agenda

- Overview
- Legislative Developments
- Recent FTC Developments
- Recent FCC Developments
- Q & A

FTC and FCC: Overview

- In the privacy and data security, advertising, and endorsements areas, there is increased activity at the federal and state level.
- Today we're going to focus on the federal level.
- Before we look at recent enforcement actions, let's look at the legislative landscape.

Recent Legislative Developments

Several important bills to be aware of:

- **Speier Federal Do Not Track Bill (H.R. 654)**
  Would require the FTC to establish standards for an online opt-out mechanism that would allow consumers to "effectively and easily" prohibit the collection or use of any "covered information"; would not pre-empt state laws; no private right of action but state AGs could enforce; would require notice of privacy practices; would allow, but does not require, FTC to establish rules for consumers to access their data.

- **Rockefeller Federal Do Not Track Bill (S. 913)**
  Establishes the framework for a "Do-Not-Track" legal obligation that allows individuals to indicate their preference to not have their online activities – including online mobile activities – tracked and, with limited exceptions, prohibits online providers from collecting personal information from individuals who indicate such a preference; also establishes that providers may continue to collect personal information from individuals who have utilized the Do-Not-Track mechanism if such collection is (1) necessary to provide a service requested by the individual and the information is anonymized or deleted as soon as that service is provided, or (2) the individual is given clear notice on the collection and use of such information and affirmatively consents to that use.

California also introduced a state Do Not Track Bill (S.B. 761)

LOEB & LOEB LLP

Recent Legislative Developments
(continued)

Several important bills to be aware of:

- **Kerry-McCain Federal Privacy Bill (S. 799)**
  Would require notice, opt-out for covered information and opt-in for sensitive information; does not contain a do not track requirement; would require covered entities to allow consumers to access and correct their personal information; authorizes FTC to develop safe harbor program; no private right of action; pre-empts some state laws; applies to covered entities that collect, use, transfer or store covered information concerning more than 5,000 individuals during any consecutive 12-month period

- **Stearns-Matheson Federal Privacy Bill (H.R. 1528)**
  Would require notice and opt-out from the sale of personal information; would allow safe harbor program; full pre-emption of state laws; no private right of action; would apply to entities that collect or sell personally identifiable information from more than 5,000 individuals during any consecutive 12-month period

LOEB & LOEB LLP

Recent Legislative Developments
(continued)

Several important bills to be aware of:

- **Markey-Barton "Discussion Draft" of Children's Privacy Bill**
  Would amend Children's Online Privacy Protection Act (COPPA) by expanding it to cover mobile devices; would create new privacy rights for children age 13 – 18; would prohibit targeted marketing of minors

- **Rush Federal Security Breach Notification Bill (H.R. 1707)**
  Would require businesses to notify individuals if their electronic unencrypted personal information is breached and implement data security programs, or face penalties of up to $5 million; includes additional data security requirements for data brokers; would pre-empt state breach notification laws, thereby creating uniform national standards

LOEB & LOEB LLP

Selected Laws, Rules And Guidelines Enforced by the FTC and FCC

- **FTC**
  - The FTC Act - Section 5 of the Act prohibits unfair and deceptive acts or practices in commerce
  - CAN-SPAM
  - Children's Online Privacy Protection Act
  - Gramm-Leach-Bliley Act
  - Do Not Call Implementation Act
  - Credit CARD Act
  - Safeguards Rule
  - Telemarketing Sales Rule
  - Guides Concerning the Use of Endorsements and Testimonials
  - Guides for the Use of Environmental Marketing Claims (aka the "Green Guides")
  - Mail Order Rule
  - Negative Option Rule

Selected Laws, Rules And Guidelines Enforced by the FTC and FCC *(continued)*

- **FCC**
  - Telephone Consumer Protection Act
  - Customer Proprietary Network Information Rules
  - Sponsorship Identification Rules
  - Children's Programming Rules
  - Truth in Billing Rules (telephone "cramming")

FTC Regulatory Developments

- **Data Security**
  David C. Vladeck, Director of the Bureau of Consumer Protection at the FTC, testified before Congress on May 4 about data security and recommended that Congress pass (1) federal security breach notification legislation, and (2) legislation that would require companies to implement reasonable security policies and procedures.

- **Mobile privacy**
  Jessica Rich, Deputy Director of the FTC's Consumer Protection Bureau, testified yesterday before a Senate subcommittee on mobile privacy. Rich stated that "the Commission is committed to protecting consumers' privacy in the mobile sphere" by bringing enforcement actions where appropriate and "by working with industry and consumer groups to develop workable solutions that protect consumers while allowing innovation in this growing marketplace." Rich also stated that the agency has "a number of active investigations into privacy issues associated with mobile devices, including children's privacy."

LOEB & LOEB LLP

FTC Regulatory Developments
(continued)

- **Privacy**
  - In December 2010, the FTC issued a privacy report, proposing a new "framework" for the collection and use of consumer information, including the development of a Do Not Track program relating to online tracking.
  - In the report, the FTC states that industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection. The FTC specifically addresses the inadequacy of privacy notices that are difficult for consumers to understand and sometimes difficult to find.
  - The FTC Report also proposes providing consumers with reasonable access to the data that companies maintain about them.

- **Unauthorized Third-Party Billing**

  The FTC held a public forum yesterday on telephone "cramming" and unauthorized third-party billing

LOEB & LOEB LLP

FTC Regulatory Developments
(continued)

- **Children's Privacy**
  The FTC is currently reviewing its Children's Online Privacy Protection Act Rule (COPPA Rule) to determine, among other things, whether it should be updated to apply to new technologies including mobile marketing and interactive gaming.

- **Environmental Marketing Claims**
  The FTC is currently reviewing its Green Guides which provide guidance for claims about environmental impact or ingredients. In October 2010, the FTC proposed revisions that relate to marketing claims that are already addressed in the current Guides, as well as claims that were not common when the Guides were last reviewed in 1998, such as "renewable energy" claims, "renewable materials" claims, and "carbon offset" claims. The FTC is expected to issue a final version of the Green Guides later this year.

- **Marketing to Kids**
  Last week the FTC issued, along with other federal agencies, guidelines for marketing food to children to combat childhood obesity.

Recent FTC Enforcement Actions

Privacy

- **Opt-Out**
  - Chitika, Inc. agreed to settle charges that it engaged in deceptive advertising by tracking consumers' online activities even after they opted-out of online tracking on Chitika's website.
  - The FTC alleged that Chitika's privacy policy said that consumers could opt out of having cookies placed on their browsers and receiving targeted ads. The privacy policy included an "Opt-Out" button; customers who clicked on it activated a message that stated, "You are currently opted out."
  - According to the FTC, Chitika's opt-out lasted only 10 days. After that time, Chitika placed tracking cookies on browsers of consumers who had opted out and targeted ads to them again.

Recent FTC Enforcement Actions

Privacy *(continued)*

- **Privacy Policy**
  - Google settled FTC charges that it engaged in deceptive tactics and violated its own privacy promises when it launched its social network called Buzz, which disclosed users' contacts. The FTC stated that this was the first FTC settlement in which a company agreed to implement a comprehensive privacy program to protect the privacy of consumer data. Google also agreed to independent privacy audits for the next 20 years.
  - The FTC alleged that Google violated its own privacy policy by disclosing users' contacts without permission, and Google failed to adequately describe how users' information would be disclosed.

Recent FTC Enforcement Actions
(continued)

Children's Privacy

- EchoMetrix, Inc., settled FTC charges that it failed to adequately inform parents using its web monitoring software that information collected about their children would be disclosed to third-party marketers.
- EchoMetrix sells its Sentry software to parents to allow them to monitor their children's online activities. When Sentry is installed on a computer, parents can log in to their Sentry account and view the activity taking place on the target computer, including chat conversations, instant messaging and the web history.
- According to the FTC, EchoMetrix provided to marketers childrens' online activity it collected through its Sentry software.
- The FTC charged that EchoMetrix violated federal law by failing to adequately disclose to parents that it would share the information it gathered from their children with third-party marketers. The only disclosure made to parents about this practice was a vague statement approximately 30 paragraphs into a multi-page end-user license agreement.

LOEB & LOEB LLP

Recent FTC Enforcement Actions
(continued)

Failure to Provide Reasonable Security for Data

- According to the FTC's complaint against Ceridian, a provider to businesses of payroll and other human resource services, the company claimed, among other things, that it maintained "Worry-free Safety and Reliability . . . Our comprehensive security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements."

- The FTC claimed the company's security was inadequate: among other things, the company did not adequately protect its network from reasonably foreseeable attacks and stored personal information in clear, readable text indefinitely on its network without a business need.

- These security lapses enabled an intruder to breach one of Ceridian's web-based payroll processing applications and obtain the personal information – including Social Security numbers and direct deposit information – of approximately 28,000 employees of Ceridian's small business customers.

LOEB & LOEB LLP

Recent FTC Enforcement Actions
(continued)

Failure to Provide Reasonable Security for Data *(continued)*

- Lookout Services, Inc., markets a product that allows employers to comply with federal immigration laws. It stores information such as names, addresses, dates of birth and Social Security Numbers.
- According to the FTC's complaint, despite the company's claims that its system kept data reasonably secure from unauthorized access, it did not in fact provide adequate security. For example, unauthorized access to sensitive employee information allegedly could be gained without the need to enter a username or password, simply by typing a relatively simple URL into a web browser.
- In addition, the complaint charged that Lookout failed to require strong user passwords, failed to require periodic changes of such passwords, and failed to provide adequate employee training.
- As a result of these and other failures, an employee of one of Lookout's customers was able to access sensitive information maintained in the company's database, including the Social Security numbers of about 37,000 consumers.

Recent FTC Enforcement Actions
(continued)

Failure to Provide Reasonable Security for Data *(continued)*

- Twitter settled FTC charges that it deceived consumers and put their privacy at risk by failing to safeguard their personal information.

- The FTC alleged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information and tweets that consumers had designated as private, and the ability to send out phony tweets from any account.

- As part of the settlement, Twitter must establish and maintain a comprehensive information security program, which will be assessed by an independent auditor every other year for 10 years.

Recent FTC Enforcement Actions
(continued)

Endorsements

- Legacy Learning System and its owner agreed to settle FTC charges that it deceptively advertised its guitar lesson DVDs through online affiliate marketers who falsely posed as ordinary consumers or independent reviewers.
- The FTC's endorsement guidelines require a reviewer to disclose a material connection with the seller of the product being reviewed.
- The FTC charged that Legacy Learning disseminated deceptive advertisements by representing that online endorsements written by affiliates reflected the views of ordinary consumers or "independent" reviewers, without clearly disclosing that the affiliates were paid for every sale they generated.
- Under the proposed settlement, Legacy Learning will pay $250,000. In addition, they have to monitor and submit monthly reports about their top 50 revenue-generating affiliate marketers, and make sure that they are disclosing that they earn commissions for sales and are not misrepresenting themselves as independent users or ordinary consumers. Legacy Learning also must monitor a random sampling of another 50 of their affiliate marketers, and submit monthly reports to the FTC about the same criteria.
- The FTC suggests that advertisers using affiliate marketers to promote their products should put in place a reasonable monitoring program to verify that those affiliates follow the principles of truth in advertising.

LOEB & LOEB LLP

Recent FTC Enforcement Actions
(continued)

Endorsements *(continued)*

- The FTC announced a settlement with Reverb, a company that provides public relations, marketing, and sales services to developers of video game applications, including mobile gaming apps.

- Reverb employees posted reviews about their clients' games at the iTunes store using account names that gave readers the impression the reviews were written by disinterested consumers, according to the FTC complaint.

- The company did not disclose that it was hired to promote the games and that the reviewers often received a percentage of the sales.

Recent FTC Enforcement Actions
(continued)

False Advertising

- **Lifelock, Inc.**
  Agreed to pay $11 million to the FTC and $1 million to 35 state attorneys general to settle charges that the company falsely promised complete protection against all types of identity theft.

- **Fake News Sites**
  FTC filed complaints against operators of fake news websites that promote acai berry weight loss products, alleging the sites contain deceptive claims about the product, falsely represent the news stories come from legitimate media outlets, and fail to disclose that the sites receive commissions based on sales of the products.

Recent FTC Enforcement Actions
(continued)

Text Message Marketing

- The FTC filed a complaint against an individual for allegedly sending millions of commercial text messages without consent and to numbers on the Do Not Call Registry, in violation of Section 5 of the FTC Act.

Do Not Call

- Numerous settlements with companies that called numbers on the Do Not Call Registry, including a recent settlement with a company that called numbers it had obtained from sweepstakes registry forms.

Recent FTC Enforcement Actions
(continued)

Environmental Marketing Claims

- The FTC charged that Tested Green sold worthless environmental certifications for hundreds of dollars, and falsely told more than 100 customers that its certifications were endorsed by two independent firms – which it actually owned.
- According to the FTC, Tested Green advertised, marketed, and sold environmental certifications using both the website www.testedgreen.com and mass e-mails to prospective consumers. The company's marketing claimed that Tested Green was the "nation's leading certification program with over 45,000 certifications in the United States."
- The FTC complaint alleges, however, that Tested Green never tested any of the companies it provided with environmental certifications, and would "certify" anyone willing pay a fee of either $189.95 for a "Rapid" certification or $549.95 for a "Pro" certification. After customers paid, Tested Green gave them its logo and the link to a "certification verification page" that could be used to advertise their "certified" status.
- The agency charged that Tested Green violated the FTC Act by providing the means to deceive consumers.

FCC Developments

Product Placement and Children's Television Programming

- In 2008, the FCC issued a Notice of Inquiry and a Notice of Proposed Rulemaking relating to product placement (which the agency refers to as "embedded advertising"). The agency asked for comments on product placement, including product placement in children's programming, and proposed amending existing sponsorship identification rules to require disclosures of a certain size that remain on screen for a particular amount of time. Comments were due September 22, 2008, but the agency has not issued a final rule yet.

Advertiser-Supported News Programs

- In April 2011, the FCC issued Notices of Apparent Liability against two television stations for allegedly airing news segments produced and supplied by advertisers, without disclosing that the segments were advertiser-supported.

FCC Developments
(continued)

Payola

- The FCC actively monitors and enforces its “payola” rules.
- The FCC extends its payola rules into all cable based advertising, even though the statute only addresses broadcast advertising.
- The FCC may try to extend its payola rules to online video news releases (VNR).

Discriminatory Advertising

- The FCC recently released several press releases requiring broadcasters to certify that they do not permit discriminatory advertising and requiring due diligence.
- This might be extended into agency and advertiser contracts.
- The FCC requires reporting of non-conforming contracts, to the possible embarrassment of advertisers.
- The FCC can extend its jurisdiction over third-parties by issuing “Citations”. So third-parties need to pay attention to the FCC’s rules.

LOEB & LOEB LLP

FCC Developments
(continued)

CPNI

- The FCC is vigorously enforcing the Customer Proprietary Network Information (CPNI) rules and requiring annual certifications from all carriers and VoIP providers showing that they protect CPNI, and reporting instances in which CPNI is released or CPNI is breached.
- The breaches need to be reported to the Secret Service and the FBI.
- Third-parties can reassemble CPNI from inbound 800 number records and it remains to be seen whether the FCC will issue Citations to parties reassembling CPNI.
- This issue is similar to the FTC's personally identifiable information (PII) concerns, where advertisers, publishers and browsers collect cookie data and reassemble it to identify specific persons.

Other Developments

Class Action Complaints Filed Against Twitter and Myspace for TCPA Violations

- Plaintiffs signed up to receive text messages from Twitter. Later, plaintiffs decided to terminate the text message program by texting "STOP" in response to one of the texts from Twitter. Twitter then sent a text message to plaintiffs confirming that they had opted-out of receiving future text messages.

- FCC rules interpreting the Telephone Consumer Protection Act (TCPA) prohibit sending a promotional text message unless the sender has obtained prior express consent from the recipient. The plaintiffs allege that they revoked their consent the instant they texted "STOP" to Twitter, and that the subsequent text message from Twitter confirming termination was therefore sent without consent. They also alleged that they incurred a charge for receiving Twitter's text message confirming termination.

- The Mobile Marketing Association U.S. Consumer Best Practices, which are widely followed by advertisers engaging in text message promotions, require marketers to send a text message confirming termination of a program.

LOEB & LOEB LLP

Doing Business in the Age of Enforcement: Key Areas of FTC and FCC Scrutiny in Advertising, Privacy and Targeting

Wednesday, May 11, 2011

Kenneth Florin
Partner and Co-Chair, Advanced Media and Technology Department;
Chair, Emerging Media Practice Group
kflorin@loeb.com | 212.407.4966

Walter Steimel, Jr.
Partner, Advanced Media and Technology Department
wsteimel@loeb.com | 202.618.5015

LOEB & LOEB LLP