Bloomberg Law Reports® Technology Law

Sheriffs of the Digital World – FTC's Commitment Further Bolstered, Settles with Twitter, Google (Among Others)

David Almeida, Sedgwick LLP

The Federal Trade Commission, the nation's consumer protection agency, has been extremely active in recent months ferreting out unfair or deceptive practices in digital marketing campaigns as well as in monitoring companies for potential privacy violations. For starters, the FTC recently announced an administrative settlement with Legacy Learning Systems (and its CEO Lester Smith) over Legacy's "Review Ads" affiliate marketing program. The FTC charged that Legacy's affiliate marketing campaign – by which it advertised its popular guitar instructional videos – violated the FTC Act because the affiliate reviewers falsely posed as ordinary consumers or independent reviewers. Legacy's practice, the FTC charged, was likely to deceive the public into believing the reviews were by impartial users of the instructional videos, not by paid marketers. As a result of the emergence of new media platforms, including social media, the FTC recently revised its long-standing Guides Concerning the Use of Endorsements and Testimonials in Advertising which, among other things, reiterated the FTC's position that "material connections" (sometimes payments or free products) between advertisers and endorsers – connections that consumers would not expect – must be disclosed. The requisite scope and manner of those disclosures has been a source of confusion and challenge to digital marketers.

The FTC's investigation centered on Legacy's "Review Ad" affiliates. These affiliates promoted Legacy's instructional DVDs by posting positive reviews and endorsements in articles, blog posts, comments and other digital copy that contained (often in close proximity) links to Legacy's website. The FTC took issue with many of those endorsements because they were not "independent reviews reflecting the opinions of ordinary consumers." Rather, the reviews created the impression that other (seemingly impartial) consumers thought that Legacy's videos were, among other things, "the most you can get for your money" and the "most comprehensive."

Compounding the problem, according to the FTC, was that the Review Ad affiliates' endorsements did not contain any disclosure of the affiliates' relationship with Legacy other than through inconspicuous hyperlinks located at the bottom of the home pages of the affiliates' web sites. And, according to the FTC's Complaint, the deception worked; twenty-five of the "Review Ad" affiliates generated revenues for Legacy in excess of five million dollars. In order to ensure sufficient disclosures of material connections going forward, Legacy agreed to pay $250,000 and to submit monthly reports regarding its top fifty revenue-generating affiliate marketers.

The Legacy investigation is significant because it is one of the few initiated since the issuance of the revised guides in December of 2009. The clear import from these initial investigations is that an effective compliance policy setting forth the company's requirement that any of its affiliated marketers comply with the disclosure obligations is likely the best defense to an FTC inquiry. In its first investigation after issuance of the revised guidelines, the FTC elected not to pursue an enforcement action against Ann Taylor LOFT based on, among other things, LOFT's voluntary adoption of a policy stating that it would not issue gifts (or anything else of value) to online endorsers without first informing them that they must disclose them. In contrast, Legacy did not have a compliance program in place to inform its affiliates that they must make the required disclosures.

The Legacy settlement serves as a stark reminder to companies to design and to enforce a compliance program providing clear instruction to affiliate marketers regarding what they can and cannot say. Compared to traditional advertising media, consumers are much more likely to believe that blog posts or comments reflect the impartial, unbiased views of fellow consumers. However, the very quality that makes digital media so attractive for companies draws increased FTC scrutiny as well. In order to ensure the integrity of online communications and to avoid drawing the ire of the FTC, companies should require their affiliate marketers to disclose any and all material connections. One of the best ways to ensure compliance is to inform affiliates that any orders generated from non-compliant affiliates will not be processed.

Finally, companies should adopt consistent internal policies to monitor their affiliate networks. As stated by David Vladeck, Director of the FTC's Bureau of Consumer Protection in announcing the Legacy settlement "[w]hether they advertise directly or through affiliates, companies have an obligation to ensure that the advertising for their products is not deceptive." Simply put, ignorance is not bliss when it comes to online endorsements by affiliate marketers, product reviewers or anyone else.

Recent Settlements with Chitika and Twitter Signal Increased Scrutiny of Privacy Practices

In addition to ensuring the integrity of digital advertising, the FTC has also been active in policing companies' data security and collection practices to ensure compliance with their posted privacy policies. On March 14, 2011, the FTC announced a settlement of its administrative complaint against Chitika, an online advertising network. The settlement concluded an investigation into the company's alleged practice of tracking consumers' online activities after those consumers opted-out of online tracking via Chitika's website.

As alleged in the FTC's complaint, Chitika is able to facilitate targeted online advertising through the use of a tracking cookie placed on consumers' web browsers when they visit a participating network publisher's website (or where a cookie has previously been set on a consumer's browser, Chitika retrieves the cookie upon a user's return to a participating publisher's website).

Chitika's privacy policy provided consumers the ability to opt-out of its online network advertising. The FTC alleged that Chitika engaged violated Section 5 of the FTC Act because, from at least May 2008 through February 2010, the opt-out from its data collection practices was only effective for ten days. After expiration of the ten day period, Chitika began placing tracking cookies on browsers of consumers who had previously opted out and sending them targeted ads once more. The FTC charged that Chitika's practice of re-initiating tracking after ten days was misleading and deceptive because users thought that they had opted out permanently; there was no prominent disclosure regarding Chitika's ten day practice.

The settlement bars Chitika from making misleading statements about the extent of data collected as well as the extent to which consumers can control the collection, use or sharing of their data. In addition, it requires every targeted ad served by Chitika to include a link taking consumers to an opt-out mechanism that enables consumers to opt-out for at least five years. The settlement also requires Chitika to destroy all identifiable user information collected while its defective opt-out was in place. Finally, the settlement requires Chitika to alert consumers who previously tried to opt-out that such attempts were not effective for as long as they may have thought and thus they should opt-out again to avoid targeted ads.

The Chitika settlement is noteworthy because – while the terms addressing consumer disclosures are clearly remedial actions for Chitika – it provides guidance on the FTC's outlook regarding the collection of consumer information as distinguished from the frameworks established by self-regulatory programs such as the Advertising Option Icon. While its Complaint did not allege as deceptive any privacy policy statements referring to tracking being anonymous, the settlement highlights the FTC's view that the distinction between personally identifiable information and non-personally identifiable information is diminishing.

In keeping with its increased focus on privacy and consumer expectation based on representations in corporate privacy policies, the FTC recently announced that it had finalized a proposed settlement with Twitter stemming from allegations that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to consumers' personal information. The FTC alleged that Twitter deceived consumers and put their privacy at risk when, between January and May of 2009, hackers were able to gain administrative control of Twitter on two separate occasions. The FTC claimed that – despite representations in its privacy policy – Twitter failed to take reasonable data security precautions, including requiring employees to store password information in secure places, to refrain from using easily decipherable passwords and to suspend accounts after an unreasonable number of failed logins. Basically, the FTC alleged that Twitter was lax in its security precautions in violation of its privacy policy.

Under the terms of the settlement, Twitter is required to implement a comprehensive information security program reasonably designed to protect the privacy and security of non-public consumer information. In order to ensure accuracy in its statements regarding its privacy protections, Twitter is required to retain an independent auditor to conduct biennial assessments to assess whether its information security program adequately protects consumer information. Twitter is further required to make available to the FTC any privacy policy statements, consumer complaints, subpoenas or other documents relating to the allegations in the FTC's complaint or to Twitter's compliance with the settlement. Finally, Twitter must file a report regarding its compliance efforts and alert the FTC to any material change affecting its compliance obligations or ability. The settlement order is to remain in effect for twenty years and any violations could result in a civil penalty of up to $16,000 each.

Google Settlement Underscores Need to Honor Terms of Privacy Policies

Even more recently, the FTC announced that Google has agreed to settle charges that it engaged in deceptive tactics and violated its own privacy policy when it launched its social network Buzz in 2010. The proposed settlement prohibits Google from future privacy misrepresentations, requires it to implement a comprehensive privacy program to protect the privacy of consumer data and calls for independent privacy audits biannually for the next twenty years. The forward looking privacy program is a first, according to the FTC, in that the program will apply to future as well as current Google products. This "privacy by design" provision

requires Google to, among other things, designate a responsible employee for privacy matters, identify reasonably foreseeable risks that may result in the unauthorized collection, use or disclosure of consumer information, institute controls to address those risks and implement procedures to select service providers that will protect consumer privacy. Notably, the settlement also requires Google to obtain permission before changing how it shares consumer data with third parties. This requirement "applies whenever Google engages in any 'new or additional sharing' of previously collected personal information 'with any third party' for the next twenty years, not just any 'material' new or additional sharing of that information." Obtaining affirmative opt-in consent is a marked departure from Google's (and others') privacy practices which provided an opt-out consent provision.

According to the FTC's complaint, Google launched Buzz through Gmail, its popular web-based email product. Google's representations to its Gmail users led them to believe that they could choose whether they wanted to join Buzz. However, according to the FTC, the options for declining the Buzz invitation ("Turn off Buzz") were ineffectual and that statements by Google that a Gmail user would not be enrolled in Buzz were false or misleading because, in fact, users were enrolled in the service. And, for users who joined the social network, the disclosure of and the controls for limiting the sharing of personal information (including e-mail addresses) were inadequate. For instance, those Gmail users who signed up for Buzz were not informed that the identity of the individuals they emailed most frequently would be made public by default.

In addition, the FTC alleged that these practices also violated Google's own privacy policy in effect at the time, which provided that "[w]hen you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."

The FTC is focused on deceptive marketing practices and privacy concerns like never before. The FTC's recent actions indicate that it will interpret privacy policies broadly and impose considerable fines and corrective action plans when companies failed to disclose material connections or to honor their privacy representations. As a result, companies should make sure that their privacy policies are easy to understand and that they accurately reflect current practices and requirements. In addition, companies should offer consumers choice when they want to use personal information for a purpose that is different than the purpose for which the information was originally collected. Finally, companies should consider incorporating "privacy by design" elements, including designating an employee responsible for privacy, training employees on privacy policies and identifying reasonable foreseeable risks to access, use, and disclosures of consumers' information that are inconsistent with the reasons for which they were provided by consumer.

David S. Almeida, a partner in the Chicago office of Sedgwick LLP, focuses his practice in the defense of consumer fraud claims, with particular emphasis on defending marketing, retail and other companies against lawsuits challenging their direct marketing practices. Almeida also counsels clients on best practices for direct, digital and mobile marketing, including advising on permission-based marketing, emerging technologies, the use of various social media platforms, as well as data security and privacy issues related to electronic and mobile commerce. He can be reached at 312.641.9050 or via e-mail at david.almeida@sedgwicklaw.com.