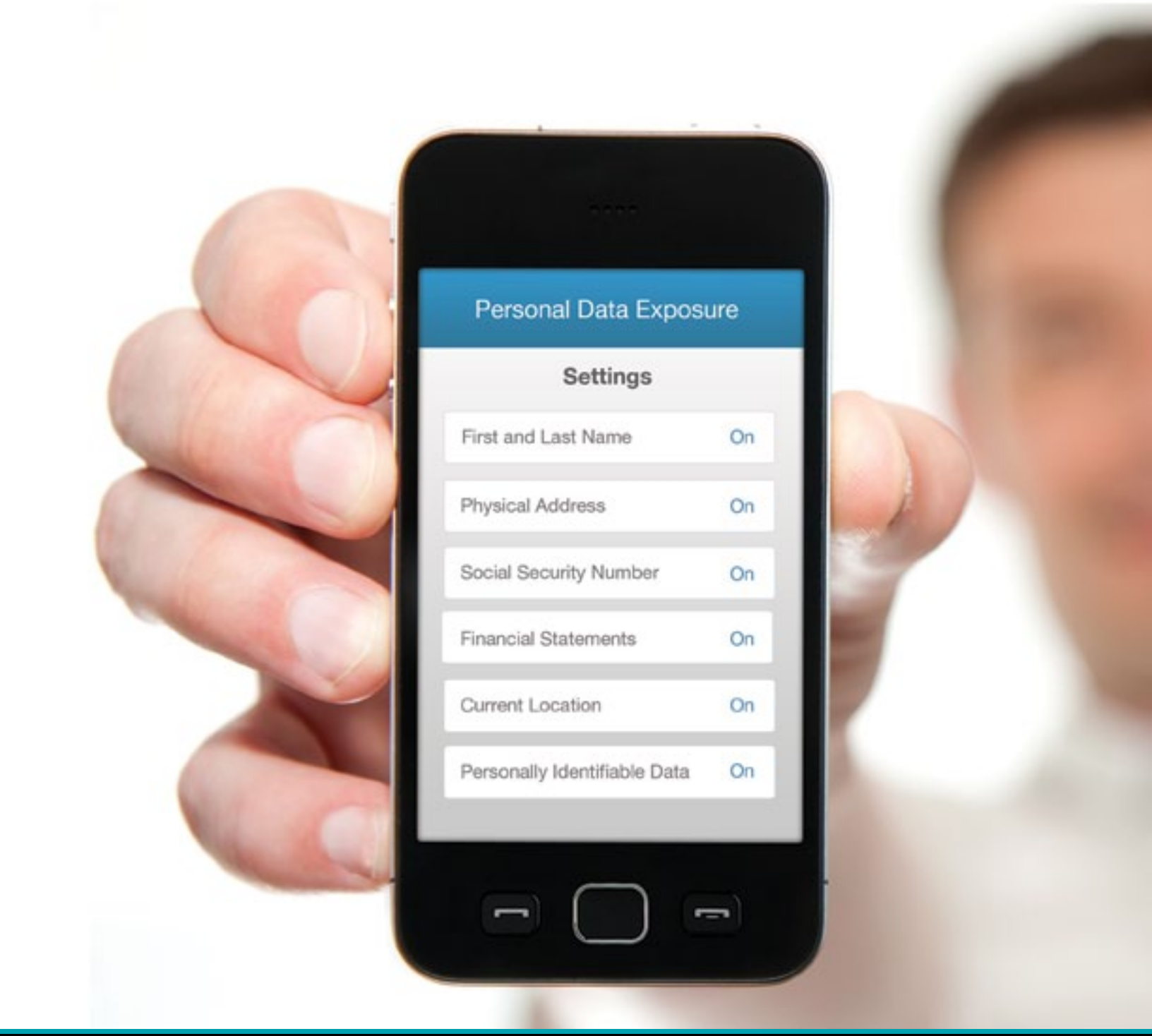
M/E INSIGHTS

ADVANCED MEDIA *WINTER/SPRING 2011*



AMEC
THE ASSOCIATION OF MEDIA & ENTERTAINMENT COUNSEL

RECENT FTC ENFORCEMENT ACTIONS INVOLVING ENDORSEMENTS, PRIVACY AND DATA SECURITY

By James Taylor & Jill Westmoreland

» ENDORSEMENTS

The Federal Trade Commission (FTC) revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising ("Guides") in December 2009 to, among other things, update the Guides with regard to social media marketing. Since the revised Guides were issued, the FTC has announced the settlements of two enforcement actions involving online reviews. Both involved reviews of products that appeared to be "independent" but were in fact provided by individuals with connections to the product's distributor. The FTC's endorsement guidelines require a reviewer to disclose a material connection with the seller of the product being reviewed.

Legacy Learning System 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 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, it must monitor and submit monthly reports about its 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 a reasonable monitoring program in place to verify that those affiliates follow the principles of truth in advertising.

The FTC announced a settlement with Reverb Communications, Inc., 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.

Under the proposed settlement order, Reverb and its sole owner are required to remove any previously posted endorsements that misrepresent the authors as independent users or ordinary consumers, and that fail to disclose a connection between Reverb and the seller of a product or service. The agreement also bars Reverb from misrepresenting that the user or endorser is an independent, ordinary consumer, and from making endorsement or user claims about a product or service unless they disclose any relevant connections that they have with the seller of the product or service.

These two enforcement actions are a reminder that the FTC is monitoring how companies market products online and, in particular, in blogs and other forms of social media. Companies that post online reviews, or engage others to post reviews, should consult the FTC's endorsement Guides. The Guides state that bloggers should disclose any material connection with an advertiser, and that endorsements should not contain false or misleading statements. The advertiser as well as the blogger can be liable for false or misleading statements made in social media. The FTC suggests that advertisers provide guidance to bloggers and should monitor blogs to see that bloggers are not making false or misleading statements. The Guides also address celebrity endorsements: celebrities can be liable for false or misleading statements, so advertisers engaging celebrity endorsers should make sure endorsers are familiar with the products and services they are promoting.

» PRIVACY

The FTC continues to be the most active regulatory agency when it comes to privacy and data collection. The FTC's primary enforcement tool is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce. For over a decade, the FTC has charged companies that fail to comply with their own privacy promises as violating Section 5 of the FTC Act.

In March 2011, the FTC announced that online advertising company 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. According to the FTC's complaint, Chitika buys ad space on websites and contracts with advertisers to place small text files (cookies) on those websites. The FTC alleged that in its privacy policy the company says that it collects data about consumers' preferences, but allows consumers to opt out of having cookies placed on their browsers and receiving targeted ads. The privacy policy includes an "Opt-Out" button. Consumers who click on it activate a message that states, "You are currently opted out."

According to the FTC, Chitika's opt-out lasted only ten days. After that time, Chitika placed tracking cookies on browsers of consumers who had opted out and targeted ads to them again. The FTC charged Chitika's claims about its opt-out mechanism contained in its privacy policy were deceptive and violated federal law. The settlement bars Chitika from making misleading statements about the extent of data collection about consumers and the extent to which consumers can control the collection, use or sharing of their data. It requires that every targeted ad include a hyperlink that takes consumers to a clear opt-out mechanism that allows a consumer to opt out for at least five years. It also requires that Chitika destroy all identifiable user information collected when the defective opt-out was in place. In addition, the settlement requires that Chitika alert consumers who previously tried to opt out that their attempt was not effective, and they should opt out again to avoid targeted ads.

In March 2011, 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 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. 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.

These are just two of hundreds of enforcement actions the FTC has initiated against companies that failed to act in accordance with their own privacy policy. Companies need to examine their data collection, use, and disclosure practices carefully. Companies that provide a privacy policy need to accurately describe their privacy practices, and update that policy to reflect any changes. In addition, companies should confirm that software or third-parties they use to process opt-outs are working properly.

» DATA SECURITY

The FTC also monitors whether companies are providing reasonable security for data they collect, store, and share. Two recent settlements highlight the importance of implementing security measures to protect employee, client and consumer data. In these actions, the FTC charged that both companies claimed they would take reasonable measures to secure the consumer data they maintained, including Social Security numbers, but failed to do so. These flaws were exposed when security breaches at both companies put the personal information of thousands of consumers at risk. The FTC challenged the companies' security practices as unfair and deceptive.

According to the FTC's complaint against Ceridian Corporation, 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.

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.

According to the FTC's press release, these two settlements are part of the FTC's ongoing efforts to ensure that companies secure the sensitive consumer information they maintain. They also illustrate the consequences of failing to provide adequate security: both companies are required to implement a comprehensive information security program and to obtain independent, third party security audits every other year for 20 years.

THE FTC PROVIDES A WEALTH OF RESOURCES RELATING TO ENDORSEMENTS, PRIVACY AND DATA SECURITY. HERE ARE JUST A FEW:

THE FTC'S REVISED ENDORSEMENT GUIDES:
What People Are Asking
http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking

SOCIAL STUDIES:
Applying the FTC's Revised Endorsement Guides in New Marketing Media
http://business.ftc.gov/documents/social-studies-applying-ftcs-revised-endorsement-guides-new-marketing-media

WHEN YOU WISH UPON A STAR:
Celebrity Endorsements & the FTC's Revised Endorsement Guides
http://business.ftc.gov/documents/when-you-wish-upon-star-celebrity-endorsements-ftcs-revised-endorsement-guides

PRIVACY POLICIES:
Say What You Mean and Mean What You Say
http://business.ftc.gov/documents/art09-privacy-policies-say-what-you-mean-and-mean-what-you-say

PROTECTING PERSONAL INFORMATION:
A Guide for Business
http://www.ftc.gov/bcp/edu/microsites/infosecurity/

AUTHOR PROFILE

JAMES TAYLOR

James Taylor is a Partner at Loeb & Loeb, Co-Chair of their Advanced Media and Technology Department, and Chair of their Advertising and Promotions Law Practice Group. Mr. Taylor's principal practice areas include advertising, promotions and privacy for advertisers, advertising and promotion agencies, and entertainment, media, Internet and mobile clients. Mr. Taylor counsels clients on their integrated marketing initiatives, agency services agreements, sponsorships and brand integration agreements, vendor and strategic partnership contracts, talent and music agreements, guild issues, social media initiatives, privacy issues including behavioral targeted marketing and data protection policies, software and technology licenses, intellectual property counseling, copy review, sweepstakes and other promotional offers. Mr. Taylor is on the Editorial Board of the Advanced Media & Technology Law Blog.

Contact: Jtaylor@loeb.com

AUTHOR PROFILE

JILL WESTMORELAND

Jill Westmoreland is an attorney at Loeb & Loeb with experience in the entertainment and publishing industries. Ms. Westmoreland conducts legal research and writes summaries of judicial decisions, legislation, regulations, enforcement actions and industry developments on a variety of topics including copyright and trademark infringement; advertising, marketing and promotions; and privacy and data security. Ms. Westmoreland is an Editor of the Advanced Media and Technology Law Blog and the Associate Editor of the IP/Entertainment Weekly Case Update for Motion Picture Studios and Television Networks.

Contact: jwestmoreland@loeb.com