Advertising Law

April 12, 2012

In This Issue

Entertainment & Media Finance Attorney Jordan Lichtman Joins Manatt

Manatt is pleased to welcome Jordan Lichtman as a partner in the Entertainment & Media practice based in the firm's Los Angeles office. Mr. Lichtman focuses his practice on all aspects of entertainment and media financing, counseling clients on the full breadth of film, television and video game production processes. He has advised clients on numerous transactions, including feature film slate financings and distribution arrangements, library acquisitions, studio co-financing transactions, second lien facilities, bridge financings and asset-backed securitizations.

back to top

FTC Settles with RockYou for Alleged Privacy Violations

The Federal Trade Commission announced a proposed settlement with online gaming company RockYou, which allegedly failed to maintain data security for its users and violated provisions of the Children's Online Privacy Protection Act ("COPPA").

In accordance with the settlement agreement, RockYou is required to (1) pay a $250,000 civil penalty, (2) implement and maintain a data security program, (3) submit to security audits by independent third-party auditors every other year for 20 years, and (4) delete information collected from children under age 13.

In addition, the company has been barred from future deceptive claims regarding privacy and data security and future violations of the COPPA Rule.

RockYou is a developer of social games and advertising solutions for purposes of social media. In 2009 the company suffered a serious data breach that exposed personal data of 32 million child and adult users to hackers. As a result, tens of millions of login details, including those belonging to minors, were stolen and published online.

While RockYou's Web site, rockyou.com, is currently used by most consumers for social games, including the popular Zoo World, at the

Newsletter Editors

Linda A. Goldstein
Partner
Email
212.790.4544

Jeffrey S. Edelstein
Partner
Email
212.790.4533

Marc Roth
Partner
Email
212.790.4542

Practice Area Links

Practice Overview
Members

Upcoming Events

April 19-20, 2012
PLI Information Technology Law Institute 2012
Topic: "Social Media Issues in Technology"
Speaker: Marc Roth
San Francisco, CA
New York, NY
For more information

May 4, 2012
New York City Bar Association's Sweepstakes, Promotions, & Marketing Laws: Comprehension & Compliance Seminar
Topic: "Mobile Marketing—Certainties & Uncertainties"
Speaker: Marc Roth
New York, NY
For more information

May 5–9, 2012
INTA's 134th Annual Meeting
Topic: "Social Media—An Ever Changing, Challenging and Competitive World: How to Provide Legal and Business Advice to Clients"
Speaker: Linda Goldstein
Washington, DC
For more information

May 7-8, 2012
ERA Government Affairs Fly-In 2012
Speaker: Linda Goldstein
Washington, DC
For more information

May 17, 2012
Response Expo 2012
Topic: "Counterfeits, Knockoffs and Digital Reputation Management"
Speaker: Linda Goldstein
San Diego, CA
For more information

July 24–27, 2012
15th Annual Nutrition Business Journal Summit
Topic: "NBJ State of the Industry"
Speaker: Ivan Wasserman
Dana Point, CA
For more information

Awards

time of the security breach the site largely focused on photo-sharing and slideshow creation tools. In order to utilize these services, users—including children—were required to register with the site by entering their date of birth, email address, and password. Once registered, users of any age were able to "create personal profiles and post personal information on slide shows that could be shared online."

At the heart of the allegations against RockYou is the question of what it did—or didn't do—with the personal information collected from its pre-breach users at the time of registration. Although RockYou promised in its privacy policy to implement reasonable and appropriate measures to protect against unauthorized access to the personal information of its users, RockYou allegedly failed to take any measures to secure, obfuscate, or encrypt the data, instead leaving it in plain text. As a result, once hackers breached RockYou's servers, they were able to easily view, steal, and publish the login details of its users.

The FTC's COPPA Rule requires Web site operators to notify parents and obtain their consent before collecting, using, or disclosing personal information from children under 13. The Rule also requires that Web site operators post a clear, understandable, and complete privacy policy. According to the FTC's complaint, RockYou violated the COPPA Rule by:

- Not spelling out its collection, use, and disclosure policy for children's information.
- Not obtaining verifiable parental consent before collecting children's personal information.
- Not maintaining reasonable procedures, such as encryption, to protect the confidentiality, security, and integrity of personal information collected from children.

Although RockYou promised in its privacy policy that it would not collect personal information from children and would promptly delete any such information once it became aware, of the 32 million RockYou accounts that were compromised by hackers in 2009, approximately 179,000 were identified as belonging to children under the age of 13. As a result of the company's failure to abide by its own privacy policy, the FTC charged that RockYou committed a deceptive act under the FTC Act.

To read the complaint in full, click here.

To read the FTC's consent decree, click here.

Why it matters: According to the FTC, the case against RockYou is part of the an ongoing effort "to make sure companies live up to the privacy promises they make to consumers, and that kids' information isn't collected or shared online without their parents' consent." In an effort to enforce data privacy, the FTC has thus far taken action against 36 companies and organizations that, like RockYou, have not taken data security seriously. Businesses that collect user information should review and, if necessary, update their privacy policy to ensure no one—including hackers—can access consumer data. In addition, organizations

should heed the FTC's warning and take the necessary steps to comply with their own privacy policy.

back to top

To Pin or Not to Pin…That Is the Question

Millions of people have flocked to Pinterest.com in the latest craze of social media sites. And it is not just individual users taking an interest—businesses are also finding significant value in using this virtual billboard to promote their brands.

Although not designed to be a business tool, retailers and businesses—especially those with a visual appeal—are flocking to the site and setting up "pinboards" to promote their brands. Whole Foods, the Cooking Channel, Pottery Barn Kids, and the Humane Society of New York are just a few of the businesses that are utilizing Pinterest to appeal to consumers.

Individuals and businesses that use Pinterest post and share their interests through a virtual collection of videos and images either found online or uploaded from the user's own personal files. Users "pin" images and/or videos onto their own pinboard, which allows them to be easily shared with others. Viewers who like a particular pin may "repin" the picture or video onto their own pinboard. If a pin originated from another Web site or pinboard, a viewer can access the original site by simply clicking on the image or video.

Through its unique online service, Pinterest has enjoyed incredible growth in recent months. But with growth also comes potential legal hassles. Specifically, since Pinterest users often post photos on their pinboards without ownership of the copyright to the image, questions have arisen about the potential for infringement of copyrights and other intellectual property rights of others. In response, Pinterest stated that it is protected under a safe harbor of the Digital Millennium Copyright Act ("DMCA"). As for concerns that its users could be liable for infringement, Pinterest downplays them, stating that the feedback from content creators has been very positive—largely because Pinterest drives traffic back to the original Web sites.

Since it does not offer advertising or paid placements, and bans "commercial use" of the site, Pinterest currently has limited uses for businesses. Nonetheless, advertising through the use of pinboards is gaining popularity. In the past few months hundreds of companies have used Pinterest to create branded profiles. Nonetheless, companies looking to use Pinterest as a forum for social media advertising must carefully consider the copyright laws before setting up their pinboard.

To allay some of these legal concerns, Pinterest has updated its Terms of Service, effective April 6, 2012. The new Terms of Service no longer allow Pinterest the right to sell a user's content and also provide improved procedures for users and copyright owners to notify Pinterest of copyright infringement. Now anyone may submit a DMCA Notice of Alleged Infringement to Pinterest, so long as the notice identifies both the copyrighted work that may have been infringed as well as the infringing content that must be removed. Pinterest has even created a simple online form that users may fill out to submit the Notice.

In its updated Terms of Service, Pinterest also changed its Pin Etiquette in an attempt to further quell any claim that the site is a vehicle for copyright infringement. Pinterest previously instructed users not to use the site "purely as a tool for self-promotion," a statement that was arguably contrary to Pinterest's general rule that users should not pin images or products they do not own or have permission to use. Pinterest deleted the above language and revised its Pin Etiquette, telling users to "Be Authentic" by pinning items that express who they are.

The question remains as to whether these changes will reduce the Pinterest user's risk of copyright infringement. While they may help limit Pinterest's liability under the safe harbor provisions of the DMCA, they may not provide enough protection for individual or business users who post content on the site. First, businesses that pin images of their own products run virtually no risk of violating copyright laws, as they generally own the images. Businesses expose themselves to potential copyright infringement if they do not own the photos of their products and do not have permission to use them. And while the Terms of Service prohibit commercial use of its Web site, there is little incentive for Pinterest to close down business-branded pinboards, since these businesses pin images of their own products. Businesses also have an incentive to do so to drive traffic to their Web sites to sell more products.

Businesses selling services have a greater risk of potential exposure than those companies that sell products. Indeed, if a small car-rental business posts images of vehicles it does not own or have permission to use, it exposes itself to copyright infringement. This is why it is critical for businesses to pin only photos to which they own the copyright or ensure they have permission from copyright owners to use theirs. Pinterest arguably minimizes its own exposure for such posts by relying on the safe harbor provisions provided to online service providers under the DMCA. In this regard, Pinterest requires users to post only User Content they own or have permission to use, and now gives any user the ability to submit a DMCA Notice for any perceived copyright violations.

Aside from potential exposure, businesses must consider whether they wish to give Pinterest permission to use their pinned images. Under the Terms of Service, Pinterest has the right to re-pin or post any User Content on Pinterest's Web site. The phrase "User Content" is broadly defined as essentially anything that a user posts or pins. So if a household name like Macy's pins images of products in its department store, Pinterest may re-pin these images. This concern seems relatively insignificant—especially for any business pinning its products that wishes to increase sales. Pinning and re-pinning images of their products means businesses enjoy access to millions of people using Pinterest, because their branded pinboards help drive traffic to their own sites—the more re-pinning, the merrier.

Individual users similarly run the risk of posting infringing content if they do not own or have permission to use the images they post. Assume a user is an avid connoisseur of Pepsi products and, in an effort to be authentic and to express herself, posts an image of her favorite Pepsi drink with comments about how much she loves it. Without

permission from Pepsi, the likely copyright holder, to pin these images, she would be posting arguably infringing content. Practically speaking, however, Pepsi most likely would not mind if users pin its products on Pinterest's site, since this promotes Pepsi's branding by driving traffic to its own Webs site. On the flip side, some businesses may not welcome any assistance with branding their products. For example, Apple may not want millions of users pinning images of their favorite iPhones on the site. But these are the risks users assume if they post images they do not own or have permission to use on the site.

Depending on the statements a user posts with pinned images, he or she may have a fair use defense under the Copyright Act. Based on a long line of court cases, Congress essentially codified the fair use doctrine under the Act. When assessing whether a defendant engaged in fair use, courts typically consider the purpose for using the content (commercial versus nonprofit or educational purposes); the type of copyrighted work involved; the portion used in relation to the copyrighted work as a whole; and the effect of the use on the potential market for, or value of, the copyrighted work. Fair use may include criticism, comment, news reporting, teaching, scholarship, and research. Unfortunately, however, there is no precise, measurable test for fair use, and oftentimes it is difficult to differentiate between fair use and infringement.

To read Pinterest's Terms of Use, click here.

To read about Pinterest's Pin Etiquette, click here.

To view Pinterest's copyright policy and complaint form, click here.

Why it matters: Pinterest is an increasingly popular social networking site for users to share content with each other. While Pinterest has updated its Terms of Use and other policies to reduce claims that the site promotes copyright infringement, individual users and businesses alike must continue to be careful about what they place on their pinboards. Pinterest has the potential to be a great marketing tool for businesses that wish to pin their products and services online in an attempt to help drive traffic to their own Web sites and increase sales. However, to avoid potential legal action, businesses must ensure they are using images they either own or have permission to use. Businesses also have to decide for themselves whether they should clamp down on users pinning photos of their products on the users' pinboards or encourage such behavior. Similarly, users should place only images they own (photos they have taken, for example) or have permission to use on their pinboards, in order to avoid exposing themselves to copyright infringement. Keeping their posts unrelated to any commercial use may also help support a fair use defense if a claim arises.

back to top

Were Those Jeans Really "Born in the USA"?

The Federal Trade Commission has closed its investigation into the legality of advertising claims made by Lucky Brand Dungarees, Inc.

The FTC initiated the inquiry in an effort to determine if Lucky Brand's

claims that its clothing is “hand crafted in America,” “born in America,” and “made in the United States” were made in violation of the FTC Act.

Prior to the conclusion of the investigation, however, Lucky removed all “hand crafted in America” and “born in America” references, and corrected statements claiming that its products were “made in the United States.”

The FTC’s inquiry into Lucky Brand’s advertising practices highlights the FTC’s authority to enforce “Made in the USA” claims under Section 5 of the Federal Trade Commission Act. Under federal law, any company making claims that its products are “Made in the USA” or “Made in America” must do so in a manner consistent with FTC decisions, orders, and rules. To help businesses understand and comply with the law, the FTC has adopted an Enforcement Policy Statement on U.S. Origin Claims and has published the guidelines entitled “Complying with the Made in USA Standard.”

When claiming a product is “Made in the USA,” the product must be “all or virtually all” made in the United States, which includes the 50 states, Washington, D.C., and all U.S. territories and possessions. Under this standard, “all significant parts and processing that go into the product must be of U.S. origin.” Should the FTC inquire about an unqualified claim, the burden of proving its accuracy falls onto the advertiser. As such, an advertiser must have a “reasonable basis” to make the claim that was supported by competent and reliable evidence.

The FTC considers various factors when evaluating unqualified claims, including whether or not the advertiser made the final assembly and processing in America. It also determines what portion of the product’s total cost is attributable to U.S. parts and processing, and how far removed any foreign content is from the final product. Advertisers are encouraged to use the cost of goods sold or the inventory costs of finished goods when analyzing whether the total cost and processing were in the United States. In this regard, manufacturers should be careful when relying on information the supplier provides about the domestic content or components in the product. The FTC notes that it is prudent to ask manufacturers for specific percentages of the U.S. content in the parts or products supplied prior to making a claim that the parts or products originated in the United States.

Advertisers may also make qualified claims that their products are “Made in the USA.” These claims denote the extent to which the product is made in America and are appropriate when the product partially contains U.S. content or processing, but falls short of a legal, unqualified claim. The FTC’s guidelines contain a few examples, including “60% U.S. content,” “Made in USA of U.S. and imported parts,” or “Couch assembled in USA from Italian Leather and Mexican Frame.” The FTC recommends that qualified claims should only be used if significant U.S. components or processing are prevalent. Otherwise, such claims might be deemed unlawful.

According to the FTC, Lucky Brand used implied claims like “Born in America” and “Hand Crafted in America.” The FTC did not, however, say whether Lucky Brand’s implied claims gave the net impression that the products at issue were made in America, nor did the FTC finalize the investigation into the truth of Lucky Brand’s express claim that its

clothing was “made in the United States.” Instead, once the FTC determined that Lucky removed all references of “hand crafted in America” from its Web site, and corrected false “made in the United States” claims on products, the FTC closed its investigation.

To read the FTC guidelines, “Complying with the Made in USA Standard,” click here.

To read the FTC Enforcement Policy Statement on U.S. Origin Claims, click here.

To read the FTC’s closing letter to Lucky Brand Dungarees, click here.

Why it matters: The FTC’s inquiry into Lucky Brand’s claims reminds advertisers to be cautious when advertising products as being “Made in America.” Advertisers must have a reasonable basis to make such claims, supported by competent and reliable evidence. While advertisers may use qualified claims, they must tread lightly so as to not overstate the truth. In addition, advertisers must be careful to revisit these issues when they bring new products into their inventory and/or change suppliers or manufacturers to ensure that existing ad campaigns maintain their truthfulness. Otherwise, an advertiser may unexpectedly find the FTC knocking on its doors.

back to top

FTC Slams the Phone on Deceptive Dialing

Telemarketers beware: The Federal Trade Commission has waged war on deceptive robocalling operations, and it is not backing down.

Just five days after shutting down a California-based telemarketing company responsible for making 2.6 billion robocalls over a 20-month period, the FTC has knocked out another group of deceptive dialers. Only this time, a federal judge in Rochester, New York, ordered the individuals behind the robocall scheme to pay $30 million in civil penalties—the largest amount ever imposed for violating the guidelines of the Do Not Call Registry.

According to a Decision and Order issued March 23, 2012, by the U.S. District Court for the Western District of New York, Paul Navestad and Christine Madpakorn, under the guise of the “Cash Grant Institute,” made over eight million robocalls to consumers. The calls falsely claimed that consumer “cash grants” were readily available from the government, private foundations, and wealthy individuals. The robocaller told consumers that since they already qualified for these grants, they could receive up to $25,000. Of the eight million calls defendants made, more than 2.7 million were made to numbers on the national Do Not Call Registry.

After enticing consumers with promises of big money payouts, the robocall directed interested parties to requestagrant.com, a Web site which, because of its ties to Navestad and Madpakorn, contained the same deceptive claims previously made by the robocaller. Cashgrantsearch.com, another Web site operated by defendants, was also referred to consumers. Unlike requestagrant.com, however, it contained images of President Obama and the Capitol Building, and asked interested parties if they were aware that “grant money exists for

almost any purpose and does not need to be repaid?"

Of course, as the FTC pointed out to the court, government "cash grants" for any purpose are pretty much nonexistent right now. And as for the Web sites to which consumers were referred, none of them actually provided grants. Instead, they referred consumers to other grant sites that provided general information about how to obtain cash grants from public or private sources for a fee. Unfortunately, consumers did not discover the truth about the grants until they paid the requisite fee to the defendants.

The FTC filed the case against Navestad and Madpakorn in July 2009, alleging violations of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce," and the Telemarketing Sales Rule, which, among other provisions, prohibits calls to consumers on the "Do Not Call List." Shortly after the filing, the court halted the defendants' operation, froze their assets, and appointed a receiver to oversee the business pending litigation. The court subsequently held that the FTC had more than enough evidence "supporting each and every element" of the complaint. In addition to imposing the $30 million penalty against defendants, the court permanently banned them from marketing grants, grant-procurement goods or services, and credit-related products, from misrepresenting any good or service, and from violating the Telemarketing Sales Rule in any fashion in the future. In addition, the court orders bar the defendants from selling or otherwise benefitting from customers' personal information, and require them to properly dispose of customers' personal information within 30 days.

The court order against Navestad and Madpakorn came down just five days after the FTC shut down California-based SBN Peripherals, a robocall company accused of placing over 2 billion illegal prerecorded phone calls pitching a variety of services, including inferior extended auto service contracts and worthless debt-reduction programs. In accordance with its settlement with the FTC, SBN Peripherals was ordered to cease telemarketing operations and hand over $3 million in assets.

According to the FTC, SBN Peripherals, operating as off-shore company Asia Pacific Telecom, scammed consumers by falsely claiming to have urgent information regarding an individual's credit card or auto warranty in a prerecorded phone call. Upon hearing this information, consumers were prompted by the robocall to press "1" for more information. Those who did were transferred to a live telemarketer who allegedly used deceptive practices to sell worthless services. Of the 2.6 billion such robocalls SBN Peripherals made between January 2008 and August 2009, 1.6 billion consumers answered the phone, and 12.8 million were connected with a sales agent.

As alleged in the FTC's May 24, 2010, complaint, defendants' actions, like those of Navestad and Madpakorn, violated the FTC Telemarketing Rules by:

- Using robocalls to contact consumers without first obtaining the consumer's written permission as required under the FTC's Telemarketing Sales Rule (effective September 1, 2009, nearly all prerecorded calls are illegal absent written consent of the consumer).
- Calling consumers whose telephone numbers appear on the National

Do Not Call Registry.

- Failing to connect to a live person when a consumer answers at a higher rate than permitted under law (three percent of all calls made).
- Continually calling consumers who have asked to be placed on the company-specific do-not-call list.

In addition, the FTC accused SBN Peripherals of making it extremely difficult for consumers to identify and track down the robocaller by transmitting vague caller ID information and displaying telephone numbers registered to its shell company, Asia Pacific Telecom.

Under the proposed settlement order, SBN Peripherals Inc., as well as Repo B.V., Johan Hendrik Smit Duyzentkunst, and Janneke Bakker-Smit Duyzentkunst, are prohibited from telemarketing, misrepresenting any good or service, and selling (or benefitting from) customers' personal information. In addition, as with Navestad and Madpkorn, defendants have 30 days to dispose of all personal information currently in their possession.

The proposed consent order was approved by the Commission in a 4-0 vote, and subsequently filed in the U.S. District Court for the Northern District of Illinois, Eastern Division, as the order is subject to court approval.

To read the Asia Pacific complaint, click here.

To read the Asia Pacific judgment and order, click here.

To read the Cash Grant complaint, click here.

To read the Cash Grant decision and order, click here.

Why it matters: In a statement, FTC Midwest Region Director C. Steven Baker said, "Telemarketers need to understand that blasting consumers with 'robocall' pitches is no longer legal.... Unless you have someone's consent up-front and in writing to receive a robocall, just don't do it. The rules could not be simpler than that, and we will go after telemarketers who ignore them." This statement emphasizes the need for businesses to routinely review their telemarketing practices with counsel and telemarketing vendors to ensure that they comply with changes in the law.

Both of these cases underscore federal regulators' ever-increasing focus on consumer privacy and their interest in affording consumers greater control over how marketing messages are delivered to them. The FTC is cracking down on schemes that target consumers who are financially strapped. Likewise, the federal government has no tolerance for individuals and companies—like Navestad and Madpakorn and SBN Peripheral—who use robocalls and other deceptive measures to defraud consumers.

back to top