Advertising Law

April 20, 2012

In This Issue

Do Not Track Is a Hot Issue With Technology Companies, Including Yahoo

Yahoo is the latest company to jump on the "do not track" bandwagon by announcing plans to implement privacy protections across its global network in the upcoming months. The service, which Yahoo says has been in development since last year, will "provide a simple step for consumers to express their ad-targeting preferences to Yahoo."

In an attempt to deliver more relevant and appealing ads to Web users, online advertisers frequently look to Web sites, such as Yahoo, Google, and Safari, to help track and analyze the Web activity of individual consumers. While financially beneficial to advertisers and the browsers that use them, tracking practices can also be useful to online users who prefer to remain logged in to sites frequently surfed, and/or appreciate receiving ads that target their specific habits.

Nonetheless, such tracking practices have recently come under the scrutiny of lawmakers and privacy advocates who believe consumers should be able to control how much of their personal data is being tracked and collected. Pointing out that some users are unaware they are being tracked, and citing concerns over the way companies use the data they collect on Internet users, privacy advocates support the use of "do not track" technology. "Do not track" allows users—such as those on Yahoo—to inform a site's servers that they don't want their activities monitored for ad-targeting purposes.

Yahoo's announcement comes just days after the Federal Trade Commission issued its final report on privacy, which urged Congress to enact general privacy legislation and recommended that companies offer consumers simpler and more obvious privacy options, such as "do not track," to allow for greater control over the collection and use of their personal data. During the House Energy and Commerce subcommittee hearing on consumer privacy earlier this month, FTC Chairman Jon Leibowitz specifically discussed "do not track," and pushed for the implementation of five significant principles, including universal implementation, ease of use, no option to override, no technical loopholes, and the ability to opt out of not just targeted ads but all behavioral data tracking.

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

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

June 12, 2012
Celesq CLE Advertising Law Webinar
Topic: "Privacy Update: Formulating Privacy Policies and Practices for Compliance with the FTC's Final Report and Guidelines"
Speaker: Jeff Edelstein
For more information

June 12, 2012
ABA Section of Litigation's 2nd Annual Food & Supplements Workshop
Topic: "So How Did Walnuts Become Drugs? Compliance Issues for Companies that Sell Supplements & Functional Foods"
Speaker: Ivan Wasserman
Downers Grove, IL
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

Although “do not track” has been around for several years, the debate between consumer privacy advocates and online advertisers recently heated up after the FTC’s privacy report was made public. Proponents of targeted advertising, including many browsers, ad networks, and other companies that track Web users’ online activity, suggest “do not track” may have grave consequences on the viability of the Internet. Online tracking is at the core of the rapidly growing online display ad market, a market that, according to online marketing firm Zenith Optimedia, is expected to grow to $34.4 billion by the end of 2012 (a projected increase of 36% from 2011). Proponents argue that the absence of targeted advertising will have a negative impact on these projected numbers. As such, Web services may not have enough advertising leverage to continue to run free of cost.

In contrast, some privacy advocates, such as the Electronic Privacy Information Center, claim that the new guidelines don’t go far enough, especially when compared to the White House’s proposed Privacy Bill of Rights, which calls for browsers to adopt an easy-to-use, streamlined “do not track” option. Others claim the answer lies not in unenforceable FTC guidelines, but rather in the passage of consumer privacy laws. At last week’s consumer privacy hearing, the FTC itself called for legislation to regulate data brokers that buy and sell personal data to help build online profiles of consumers. In addition, according to a recent *New York Times* article, Chairman Leibowitz said he would favor legislation requiring “do not track” policies if companies could not create “robust” policies themselves.

It appears the major browsers are listening. In an effort to comply with the FTC’s and the White House’s recommendations, many, like Yahoo, are taking steps to find ways to protect consumers from being tracked by Web-based marketing companies. Some, including Microsoft and Mozilla, already have “do not track” options on their servers. In 2010 Microsoft announced “Tracking Protection” in Internet Explorer 9, which allows users to subscribe to blacklists from companies such as TRUSTe and PrivacyChoice to block third-party tracking sites from placing cookies on consumers’ hard drives. Soon after, in January 2011, Mozilla came out with its “Do Not Track” technology, which allowed users to check a settings option that will send a message to sites expressing a consumer’s wish to not be tracked. Internet Explorer and Mozilla have since voiced support of the White House plan.

Google also lent support to the White House plan, pledging to “adopt a broadly consistent approach” to “do not track” technology for its Chrome browser. However, Google is moving slowly—it is not planning to make the service available to users until “the end of the year.”

Similarly, Opera said it supports the “do not track” header in its cross-platform browser core and it’s available in the alpha release of Opera 12. Although “we still harbor reservations about the Do Not Track feature, including the risk that it gives a false sense of security,” Opera stated, “we believe security and privacy on the Web should be strengthened, so we have implemented Do Not Track and remain active, committed participants in the W3C working group.”

Apple, too, offers a “do not track” option. However, since Apple earns its revenues almost entirely from hardware sales, it doesn’t have the

Awards

Recognized for Excellence in the areas of Advertising, Marketing and Media

Named a Top Practice Nationally for Marketing and Advertising

Practice leaders included among the prestigious *Best Lawyers* in the country same motivation to track users as other browsers and Internet service providers do. Even Apple's iAd network gains limited benefits from reporting user behaviors, which arguably makes it easier for Apple to offer legitimate opt-out options than others do.

To read the FTC's final report on privacy, click here.

To read the *New York Times*' recent article on "Do Not Track," click here.

Why it matters: While the issue of Web privacy and the debate surrounding "do not track" can be complicated, announcements like Yahoo's serve to remind us how important it is for privacy supporters and businesses to continue the dialog and to work together on a solution. Online privacy is a subject that will undoubtedly generate quite a bit of debate over the next few years. As such, all Web sites—even small ones—should carefully examine how they track users and store private information. Policies regarding the transparency of such information should also be scrutinized. Public opinion often fuels the level of success a Web site enjoys. As such, by voluntarily implementing privacy protections, browsers and other companies will gain credibility in the eyes of consumers and government entities.

back to top

NAD Issues Decision in Priceline Dispute

The National Advertising Division of the Council of Better Business Bureaus (NAD) has determined that Priceline.com, Inc. (Priceline) did not falsely denigrate competitor Travelocity.com LP (Travelocity) in an advertisement for Priceline's "Name Your Own Price" service for hotel reservations.

Travelocity's challenge involved a Priceline advertisement where spokesman William Shatner, featured in a spy-thriller spoof, said, "So, you've been double-crossed by other travel sites and now you want to try the real deal?" According to Travelocity, although the advertisement never mentioned the company's name, Shatner's statement implied that travelers will be deceived, betrayed, and cheated if they use Travelocity to reserve airline tickets or hotel rooms.

In its defense, Priceline insisted that the commercial did not directly or indirectly defame or disparage Travelocity. In support of its position, Priceline offered into evidence the results of a consumer perception survey that targeted individuals with prior experience using online sites to book hotel rooms. Persons who had not booked travel online were excluded from the survey on the basis that they were presumably less familiar with the online booking process. In the past NAD has raised issues with surveys, such as Priceline's, that include a very limited and narrow target population.

Since Priceline and Travelocity are not only utilized by consumers who have experience booking travel online, NAD concluded that Priceline's survey should have included inexperienced as well as experienced consumers. Without using the correct target population, the survey failed to adequately study the full range of customers for whom Priceline and Travelocity compete, thereby rendering it unreliable for purposes of NAD's review.

In cases where it cannot rely on evidence of user perception, NAD must assume the role of the consumer and independently assess the messages conveyed by a specific advertisement. After conducting an independent examination of Priceline's commercial, NAD found it did not falsely malign Travelocity. In contrast, NAD found that the advertising at issue was nothing but a lighthearted spoof. As such, NAD concluded that consumers were unlikely to come away from the advertising with the message that Travelocity and other travel sites "double-cross" their customers.

To read NAD's decision, click here.

Why it matters: NAD's review of Travelocity's claim against Priceline serves as a reminder to advertisers to carefully review implied and express claims in the context of the entire ad. In addition, advertisers need to recognize that the methods used in the collection of data are vital to the validity of use of user-perception surveys. Companies should seek legal advice when designing surveys to ensure that they meet established criteria for well-conducted surveys.

back to top

Class Action Hopes to Feast on Frito-Lay and Pepsi

In a recent federal class action lawsuit, Frito-Lay and its parent company PepsiCo were accused of violating federal and California laws by "misbranding" their potato and snack chips as healthy.

At the heart of the complaint are Frito-Lay's claims that Lay's potato chips are "prepared with healthier oils," that Frito-Lay's snack chips "contain 0 grams of Trans Fat, are low in saturated fat and cholesterol-free," and that Frito-Lay's snacks contain "good stuff like potatoes, which naturally contain vitamin C and essential minerals." Plaintiffs further allege that Frito-Lay told consumers that "Snacking is an important part of a healthy diet" and that "Snacks may benefit special populations, including people with diabetes, children and adolescents, older adults, and pregnant women."

By touting its products as healthy and neglecting to mention that Lay's chips have more than 13 grams of fat for every 50 grams, and Frito-Lay's snack foods contain high levels of fat, saturated fat, cholesterol, or sodium, the plaintiffs allege that Frito Lay's claims violated provisions of both the federal Food, Drug & Cosmetic Act and California's Sherman Food, Drug & Cosmetic Act. Under these laws, food items are misbranded if the package labeling is false or misleading, such as the omission of disclosures about the product's nutrient content. According to the class action lawsuit, "As consumer preferences have begun to favor healthier options, Defendants have chosen to implement a health and wellness strategy to reposition their products as a healthy option . . . . Defendants recognize that health claims drive food sales and actively promote the purported health benefits of their misbranded food products, notwithstanding the fact that such promotion violates California and federal law."

The Frito-Lay false advertising class action lawsuit is brought on behalf of all California consumers who within the past four years purchased Frito-Lay potato chips. The class is seeking damages, restitution or disgorgement, as well as a cease-and-desist order banning the companies from selling their allegedly misbranded food products.

To read the complaint filed in *Wilson v. Frito-Lay North America, Inc. et al.,* click here.

Why it matters: Food retailers must carefully ensure their product package labels comply with federal and state laws and regulations when making nutrient content claims. It is prudent to periodically review product labels for compliance, especially when manufacturers change the content of their products or roll out new advertising campaigns about the health benefits of these products. Indeed, the cost of prudent compliance review is insignificant in comparison to defending a class action lawsuit or an investigation by federal or state regulators.

back to top

The Digital Millennium Copyright Act's Safe Harbor May Not Be So Safe

The United States Second Circuit Court of Appeals issued an opinion on April 5, 2012, breathing new life into litigation brought by Viacom (and other entities and media companies) against Google's YouTube for alleged copyright infringement.

According to Viacom, YouTube violated copyright laws by knowingly displaying and reproducing Viacom's content on YouTube's Web site.

The United States District Court for the Southern District of New York entered summary judgment in favor of YouTube under the safe harbor provisions of the 1998 Digital Millennium Copyright Act (DMCA), which protects online service providers from being liable when users post infringing content. However, after finding that YouTube may have engaged in "willful blindness" by failing to take steps to remove the infringing content on its Web site once it found out about it, the Second Circuit vacated the District Court's order granting summary judgment and remanded the case for further proceedings.

In the underlying action, Viacom alleged that YouTube engaged in direct and secondary copyright infringement by displaying or reproducing roughly 79,000 audiovisual "clips" on its Web site between 2005 and 2008. These clips included videos from *The Daily Show with Jon Stewart*, *South Park*, *SpongeBob SquarePants* and other programs. YouTube claimed it was not liable under the DMCA's safe harbor provision, which covers any infringement claims arising "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." Since users posted the clips, YouTube claimed it had safe harbor protection.

The District Court found that since YouTube had insufficient knowledge about the infringing activity, the safe harbor provision did apply. In reaching its decision, the District Court stated that safe harbor protection would not apply if the online service provider had "knowledge of specific and identifiable infringements." As such, the District Court concluded that the provider must have "item-specific knowledge of [the] infringing activity" for the provider to have the "right and ability to control" infringing activity under the DMCA. The District Court further held that "replication, transmittal, and display of videos on YouTube constituted activity 'by reason of the storage at the direction of a user' within the meaning of the law."

The Second Circuit found that while the District Court properly held that safe harbor requires knowledge or awareness of specific infringing activity, the issue of whether or not YouTube "had actual knowledge or awareness of specific infringing activity on its Web site" is factual, and therefore should be determined by a jury. However, the Second Circuit also concluded that the District Court erred by requiring YouTube to have item-specific knowledge of infringing activity under the "right and ability to control" provision of the law in order for it to be liable. Instead, according to the evidence, consisting of surveys and an opinion by Google's financial advisor (Credit Suisse), about 60% to 80% of YouTube's content may have been copyrighted material.

Evidence of internal communications and reports further indicated the possibility that YouTube had knowledge of infringing activity on its Web site. E-mail communications between YouTube's founders contained discussions of infringing content – Bud Light commercials and CNN video clips of the space shuttle – on their Web site, which one founder recognized as "blatantly illegal." Since YouTube was still relatively new at the time, the company decided to leave them up longer so the site could gain more publicity. Evidence suggests YouTube's founders considered that it could take the copyright owners a couple of weeks to discover the videos, and issue cease-and-desist orders, at which point YouTube would remove them. Based on the evidence, the Second Circuit concluded that a jury could find YouTube had "actual knowledge of specific infringing activity, or was at least aware of facts or circumstances from which specific infringing activity was apparent." Summary judgment in favor of YouTube was therefore deemed premature.

The Second Circuit also considered the application of the common-law doctrine of "willful blindness" in the context of the DMCA as a matter of first impression. Under the doctrine of willful blindness, a business or individual is "willfully blind" when "aware of a high probability of the fact in dispute and consciously avoided confirming that fact." When found willfully blind, the business or entity is deemed to have knowledge of the fact. Nothing in the DMCA "abrogates" the doctrine. The Court, therefore, found that the doctrine could demonstrate knowledge or awareness of specific instances of infringement. And based on the evidence, a question of fact remained whether YouTube intentionally made an effort to "avoid guilty knowledge" of infringing content on its Web site.

In conclusion, the Second Circuit held that the "right and ability to control" infringing activity under the DMCA requires "something more" than just the ability to remove or block access to materials on the provider's Web site. The Court noted, however, that defining the "something more" is difficult, but nonetheless rejected the District Court's conclusion that specific knowledge of the infringement was required. Ultimately, the Second Circuit remanded the issue for the District Court to determine if there was sufficient evidence for a jury "to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity."

To read the decision of the United States Court of Appeals for the Second Circuit, click here.

Why it matters: The Second Circuit's decision sends a strong message to Internet and online service providers that safe harbor under the DMCA is not an absolute blanket of protection. If there is any evidence that such providers had actual knowledge of infringing content on their Web sites, they may have liability exposure for copyright infringement. In order to stave off potential liability from copyright owners, it is therefore critical for any service provider to ensure that it removes any infringing content immediately after learning of its existence. The belief by YouTube's founders that leaving protected content on their Web site for a little while longer to garner more publicity posed no risk to the company could prove to be a costly miscalculation.

back to top

Groupon's "Daily Deal" Proves Costly

Groupon, Inc., creator of a "daily deal" Web site, has agreed to pay $8.5 million to settle a class action lawsuit resolving claims that it violated federal and state consumer protection laws by imposing illegal expiration dates and other restrictions on the "daily deal" vouchers/coupons it offers to online consumers.

The settlement arose out of 17 class action lawsuits originally filed against Groupon in California, the District of Columbia, Florida, Illinois, Massachusetts, Minnesota, and Ohio.

These separate actions were ultimately consolidated before a federal judge in the Southern District of California. Together, plaintiffs claimed that by placing expiration dates and other provisions on their vouchers, Groupon and various related merchants violated state consumer protection laws as well as the Electronic Funds Transfer Act, as recently amended by the Credit Card Accountability Responsibility and Disclosure Act (the "CARD Act"). According to the CARD Act, gift cards with a dollar amount on them must continue to be good for no less than five years from the date of purchase. In contrast, many of Groupon's vouchers expired within 30 days of purchase.

Plaintiffs further alleged that Groupon unlawfully required vouchers to be used in a single transaction, failed to give cash refunds for unused portions, and imposed class action waivers and mandatory arbitration provisions onto consumers. In addition, by offering "daily deals" for such a limited time, plaintiffs claimed Groupon created a sense of urgency among consumers, who rushed to buy vouchers before taking notice of the expiration dates and full terms. As a result, many of these coupons were never used, which has ultimately led to an unlawful windfall to Groupon.

The proposed settlement allows class members who purchased or received Groupon coupons in the United States between November 2008 and December 1, 2011, to redeem their expired coupons or request a refund from the $8.5 million settlement fund. Although Groupon denied liability in agreeing to settle, over the next three years the company has agreed not to sell more than 10% of daily deals that expire less than 30 days after issuance (excluding certain categories like travel-related offers and admissions for ticketed events). In addition, in situations where there is a difference between the date of expiration of the promotional value and the date of the expiration of the purchase price, Groupon has agreed to make clear and conspicuous disclosures.

To read the Groupon Class Action Complaint, click here.

To read the Groupon Joint Motion Re Preliminary Approval of Settlement, click here.

To read the Groupon Transfer Order, click here.

Why it matters: The Groupon case demonstrates the importance of addressing legal issues specific to the fast-growing "daily deal" trend. To help minimize the risk of being embroiled in protracted class action litigation or regulatory enforcement proceedings brought by federal or state regulators, companies should take a close look at any offers that combine prepayment with an expiration date. Likewise, prior to enacting such offers, they should seek the advice of legal counsel to ensure offers do not violate any applicable state laws.

back to top