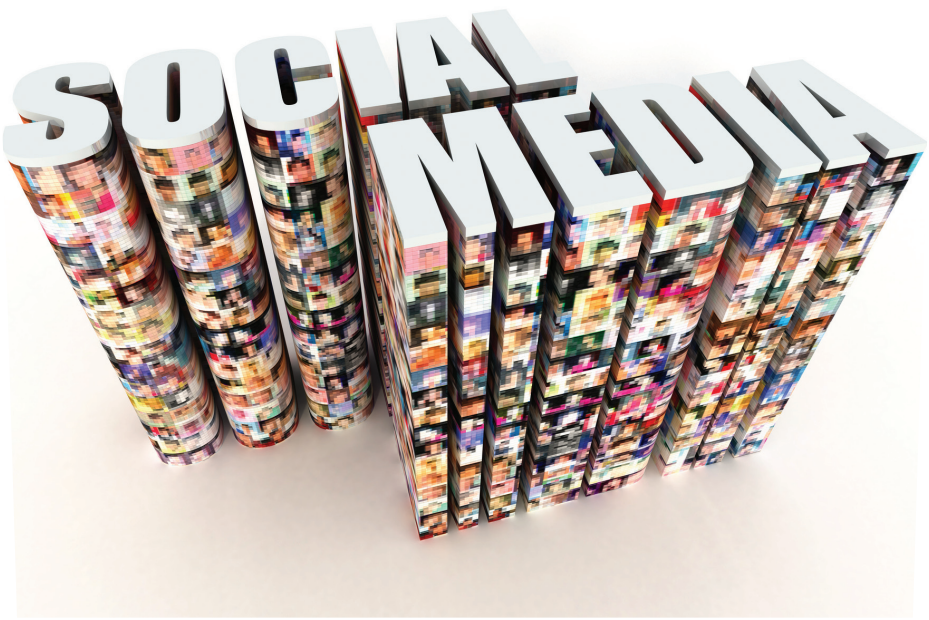
Morrison & Foerster Social Media Newsletter

Vol. 2, Issue 2 April 2011

Socially Aware:
The Social Media Law Update



In this issue of *Socially Aware*, our guide to the law and business of social media, we discuss the Federal Trade Commission's groundbreaking proposed consent order arising out of Google's ill-fated launch of its Buzz social network. We take a look at an ominous new decision suggesting that the CAN-SPAM Act may apply to communications within Facebook and other social media sites. We summarize an important Ninth Circuit decision regarding the interplay between contract law and copyright law in connection with online terms of service breaches. We highlight two new employment law developments that should be taken into account in drafting or updating your company's social media policy. We report on the EU's plans to bolster the privacy rights of social media users. We provide an overview of liability risks in the United Kingdom for online service providers hosting defamatory materials posted by others. We examine the alcoholic beverage industry's cautious embrace of social media. We provide an update on some recent developments in the Righthaven "copyright troll" lawsuits. Finally, we provide a statistical snapshot of a typical 20 minutes in the life of Facebook. Let's get started . . . .

IN THIS ISSUE

EDITORS

John Delaney
Gabriel Meister
Aaron Rubin

CONTRIBUTORS

Kara Alesi
Teresa Burlison
Seth Graham
Susy Hassan
Susan McLean
Shawn Oakley
Julie O'Neill
Karin Retzer

FTC Charges Google With Deceptive Practices; Proposed Settlement Breaks New Ground

In launching its Buzz social network in 2010, Google invited its Gmail service users to participate with two options: *"Sweet! Check out Buzz"* or *"Nah, go to my inbox."* According to the Federal Trade Commission (FTC), *each* of these choices was deceptive: those who clicked on *"Nah"* were unwittingly enrolled in certain features of the social network, while those who clicked on *"Sweet!"* were not clearly told that the identities of those they emailed most often would, by default, be made public—contrary to Google's promise to obtain consent for new information uses and allegedly in violation of the substantive requirements underlying the company's US-EU Safe Harbor certification.

Over the years, the FTC has settled numerous actions against companies that allegedly failed to keep their privacy promises by ordering them to never break their promises again. Its enforcement action against Google is different. On March 30, 2011, the FTC announced a proposed consent order that breaks new ground. Although it includes the standard injunctive relief, it goes much further in several notable ways.

First, for the first time, the FTC has imposed a *"privacy by design"* provision that requires Google to implement a comprehensive privacy program that, among other things, addresses the risks related to new products. Second, Google must undergo an independent privacy audit every other year for 20 years. These two requirements are typical of the FTC's orders resolving charges of insufficient data security measures but are new for alleged privacy violations. We expect that such provisions, going forward, will become standard in privacy orders. Third, the order requires Google to obtain users' opt-in consent before sharing their information with third parties if the sharing is contrary to any promises it has made.

We note that this is the first time that the FTC has alleged substantive Safe Harbor-related violations. It is unclear whether the proposed order's opt-in requirement is intended to go beyond Google's alleged failure to comply with its privacy policy and also remedy its alleged failure to comply with its Safe Harbor obligations. If so, the proposed order's opt-in requirement would be more restrictive than the Safe Harbor's own requirement for opt-out choice for new information uses. Parties commenting on the proposed order are expected to raise this issue, and the final order will likely provide greater clarity.

. . . for the first time, the FTC has imposed a *"privacy by design"* provision that requires Google to implement a comprehensive privacy program that, among other things, addresses the risks related to new products.

The FTC has historically signaled its expectations through its consent orders – in effect, creating a "common law" for industry to follow. The proposed Google order is no different. It puts businesses on clear notice that the FTC will continue to hold companies to their privacy and Safe Harbor promises, imposing strong injunctive relief in the case of failures. It also signals that the FTC is at least beginning to view "privacy by design" as a legal requirement.

California District Court Holds Facebook Posts Subject to CAN-SPAM Act

If your company communicates with consumers within social networking sites such as Facebook, MySpace, LinkedIn, or Twitter, take note of a recent court decision finding that the federal CAN-SPAM Act applies to more than email. On March 28, 2011, in *Facebook Inc. v. MaxBounty Inc.*, the U.S. District Court for the Northern District of California, in refusing to dismiss a CAN-SPAM Act claim arising from messages sent and received within the Facebook platform, held that the Act's restrictions apply broadly, extending beyond traditional email messages and social networking site users' inboxes to the delivery of communications to other "unique electronic destinations," including Facebook users' walls and news feeds. The decision puts marketers on notice that their communications within Facebook and other online social networks may need to comply with the Act's requirements—although exactly how to comply poses significant challenges, given that the Act predates the rise of social media and focuses on concepts that apply more easily to email messages than to pokes and tweets.

As a practical matter, our understanding is that the Federal Trade Commission does not currently intend to apply the Act to social networking activities in enforcement actions, and it would be out of character for the FTC to do so

without first providing industry with guidance. Nor is enforcement likely from state Attorneys General, particularly absent fraud or other tangible harm to consumers. Rather, we expect that both federal and state regulators will look to social networking service providers to continue to patrol their own communities for violations of their online terms of use, which generally contain strong anti-spam provisions. Bolstered by this decision, these providers are likely to continue to vigorously enforce their rights, particularly where marketers fail to honor users' preferences. Accordingly, marketers should ensure that their communications with social network users comply with the applicable networks' own rules, which may change from time to time.

EVERY 20 *MINUTES* ON FACEBOOK:

10,208,000	New comments
2,716,000	New photos uploaded
1,972,000	"Friend" requests accepted
1,851,000	New status updates
1,587,000	New wall posts
1,484,000	Event invites sent
1,323,000	Tagged photos
1,000,000	Shared links

Source: http://www.facebook.com/notes/democracy-uk-on-facebook/a-snapshot-of-facebook-in-2010/172769082761603

Ninth Circuit Takes Sides in Battle Over Terms of Use in World of Warcraft Case

The Ninth Circuit's recent decision in *MDY Industries LLC v. Blizzard Entertainment, Inc.* has important implications for online content and service providers that seek to control downstream use of their products through license restrictions contained in end-user "terms of use" and similar terms and conditions. The *Blizzard* case concerned "Glider," a software "bot" program made by defendant MDY, which automatically plays plaintiff Blizzard's Internet game World of Warcraft ("WoW") on behalf of a user, thus allowing the user to advance through skill levels and amass in-game rewards. Some WoW users complained about Glider, prompting Blizzard to amend its WoW end-user terms of use to prohibit use of the program.

The *Blizzard* case addressed a number of issues, including Blizzard's claims under the Digital Millennium Copyright Act based on MDY's distribution of a premium version of Glider intended to circumvent certain technological measures that Blizzard had introduced to block the program. For many readers of *Socially Aware*, however, the most interesting aspect of the case may be the Ninth Circuit's treatment of Blizzard's claims for contributory and vicarious copyright infringement, and the analysis of those claims in relation to Glider users' violation of the WoW end user terms of use—in particular, the court's discussion of whether the terms of use imposed merely covenants on users, rather than conditions to the existence of a user's license to access and use Blizzard's copyrighted game.

Blizzard argued that any WoW player who violated the terms of use by using Glider thereby lost his or her license to play WoW—*i.e.,* compliance with the terms of use was a condition on the player's right to play the game—and, therefore, such a player infringed Blizzard's copyrights by using Glider to play WoW. Such underlying infringement by the player, in turn, supported Blizzard's claim that MDY was liable for contributory and vicarious infringement. MDY conceded that Glider users violated WoW's terms of use, but argued that users were merely breaching covenants and not conditions of the license—that is, a user who breached the WoW terms of use did not, as a result of such breach, lose his or her license to access and use WoW. Therefore, MDY argued, there was no copyright infringement by users for which MDY could be held secondarily liable.

The Ninth Circuit held for MDY on the copyright infringement issue, finding no failure of license conditions, only breach of covenants. According to the court, for there to be a failure of a condition of a license, the conduct at issue must exceed the license's scope in a manner that implicates one of the licensor's exclusive statutory rights. The court found that the use of Glider did not implicate any of Blizzard's exclusive rights under

copyright law because Glider did not alter or copy the WoW software. For there to be infringement, the court concluded, there must be a "nexus" between the license condition and an exclusive right of copyright:

> Were we to hold otherwise, Blizzard—or any software copyright holder—could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners.

It is instructive to compare *Blizzard* to the Federal Circuit's 2008 decision in *Jacobsen v. Katzer*. In that case, the plaintiff Jacobsen owned the copyright in certain computer code that he made available for free download pursuant to an open-source license called the "Artistic License." The defendant Katzer developed commercial software products for the model train industry. Jacobsen accused Katzer of copying certain materials from Jacobsen's website and incorporating them into one of Katzer's software packages in a manner the violated the Artistic License. The Federal Circuit, in ruling for Jacobsen, held that the Artistic License imposed "conditions" that limited the scope of the copyright license. The court specifically noted that the Artistic License grants the rights to copy, modify, and distribute the software, *provided that* the applicable conditions are met; and also that, under California contract law, the language "provided that" typically denotes a condition. Additionally, the court highlighted that the terms of the Artistic License govern the manner in which the licensee is permitted to modify and distribute the material, restrictions that are directly related to the economic interests of copyright policy.

In light of *Blizzard* and *Jacobsen*, online content and service providers (and, indeed, any licensors), at a minimum, would be well-advised to include language in their terms of use and other license agreements that clearly imposes conditions on the license—*e.g.,* "Licensee may access and use the Service, *provided that* . . ." or "Subject to *and conditioned upon* compliance with this Agreement, Licensor grants to Licensee a license to . . . ." Using such language may help to support copyright infringement claims against users who breach the applicable license terms, thereby making available remedies that may not be available for mere breach of contract claims, including injunctive relief and statutory damages for willful infringement. Note, however, that *Blizzard* and *Jacobsen* reveal that courts may not always be receptive to a licensor's attempt to impose license conditions that are unrelated to the applicable underlying intellectual property rights.

New Charge Before the NLRB Strikes Out at Broadly Drawn Social Media Policies

In the past two issues of *Socially Aware*, we tracked the progress of a complaint issued by the National Labor Relations Board ("NLRB" or "Board") against an employer for terminating an employee who allegedly posted complaints about her supervisor on her Facebook page. In light of the fact that the employee's co-workers viewed and commented on her posts, the NLRB claimed that the employer had violated the employee's rights under federal labor laws to discuss her wages, hours, and working conditions with fellow employees.

As discussed in last month's issue, that case was settled privately this past February. Now, the NLRB is investigating another "Charge Against Employer" alleging unfair labor practices, NLRB Reg. 34, No. 34-CA-12906, based on similar issues but with a potentially significant twist.

Employers should keep their eyes on these and similar matters before the NLRB, in order to help ensure that their social media policies are not construed as interfering with protected employee rights.

In this new charge, filed by the Connecticut State Employees Association/SEUI Local 2001 on February 4, 2011, the employer at issue, bus company Student Transportation of America, has been charged not with terminating an employee in violation of federal labor laws, but simply with "maintaining and enforcing" an overly broad social media policy that bans "the use of electronic communication and/or social media in a manner that may target, offend, disparage or harm customers, passengers or employees," in violation of the National Labor Relations Act ("NLRA"). The charge itself does not allege that this policy has been enforced against Student Transportation of America's employees. Although the Board has yet to file a formal complaint against the employer, its next steps could help clarify whether and to what extent the mere establishment of broadly-restrictive social media policies may unlawfully restrict employees' rights.

Employers should closely monitor this and similar matters before the NLRB, in order to help ensure that their social

media policies are not construed as interfering with protected employee rights. And, as always, employers should carefully consider potential legal risks arising from disciplinary action against or termination of employees who, through social media, or otherwise, may have engaged in protected conduct under the NLRA.

First Amendment Shields Disgruntled Ex-Employee From Liability for Accusatory Website

A fired employee's explosive online accusations against his former employer are constitutionally protected speech under the First Amendment, a New York state judge recently ruled.

Cambridge Who's Who Publishing, Inc., a Long Island-based company that provides marketing and networking services to business professionals, hired Harsharan Sethi as its director of management information systems in July 2008. At the time of his employment, Sethi agreed not to use Cambridge's confidential information, including "client names, addresses, and credit card numbers," other than in carrying out Cambridge's business. After Cambridge fired Sethi in early 2010, Sethi established several websites allegedly dedicated to smearing Cambridge publicly.

As reported in Law.com, Sethi allegedly launched the first website at issue at thecambridgeregistryscam.com URL. The site stated that Cambridge customers might be entitled to a refund, encouraged customers to file legal complaints against Cambridge, and offered to expose members of Cambridge's management's lifestyles and "prior run ins" with the law and the IRS. In May 2010, Cambridge asked a New York State Supreme Court to enjoin Sethi from interfering with its customers and good will, and from maintaining any blog or website concerning his former employment with Cambridge. In September 2010, the court enjoined Sethi from soliciting Cambridge customers or divulging their personal information, but refused to restrain him from making "defamatory statements concerning Cambridge." Sethi then launched his second website, whoswhoamongscammers.com, which, although it did not mention Cambridge by name, echoed the accusations of data loss that Sethi had raised about the company with state authorities. The site further described items of customer data that allegedly had been lost, and claimed that, despite its knowing of this loss, Cambridge's management had failed to report the loss to authorities.

The *Cambridge* ruling is a reminder that, in some cases, when employee grievances involve matters of public concern, free speech principles may well hinder an employer's ability to silence them.

Cambridge made a second effort to enjoin Sethi from maintaining a blog or website concerning his former employment, which Sethi resisted on free-speech grounds—and, in its most recent decision, the court again sided with Sethi. Relying on the U.S. Supreme Court's decision in *FEC v. Wisconsin Right to Life, Inc.*, the court ruled that the alleged data loss "implicate[d] the economic interests of a large number of people" and was a matter of public concern and, accordingly, that even though Sethi's online postings may have been motivated by the intent to "disparage [Cambridge's] business" or "retaliate for [his] discharge," the core content of such postings entitled the speech to constitutional protection.

As HR departments everywhere know well, the Internet gives disgruntled employees (and ex-employees) an expansive public platform for airing grievances and, potentially, for exacting revenge. The *Cambridge* ruling is a reminder that, in some cases, when those grievances involve matters of public concern, free speech principles may well hinder an employer's ability to silence them. (Irrespective of the court's ruling, neither of Sethi's websites appears to be currently active.)

EU to Get Tough With Social Media Sites

The European Union plans to reinforce users' privacy rights on social media sites, EU Vice President and Justice Commissioner Viviane Reding announced at a March 16, 2011 meeting organized at the European Parliament. The European Commission is currently reviewing the 1995 Data Protection Directive to bring it in line with new technologies; a legislative proposal is expected in the summer of 2011.

Reding made clear that the Commission intends to introduce new laws to give users greater control over their data on the Internet. Companies operating online will be required to comply with EU privacy laws, regardless of their location: "For example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules," Reding announced in a recent press release.

At the March 16 meeting, Reding specifically addressed users' "right to

For an online social network, this would mean that all traces of information, including photographs, comments, and user profiles, would be permanently removed from the social network, as well as from any company storage.

be forgotten" online, and explained how new legislation would directly affect the way online social networks operate. Individuals would have a legal right—and not just the opportunity to request—to "withdraw their consent to data processing" and have their data permanently removed from websites, or to stop their data from being processed. For an online social network, this would mean that all traces of information, including photographs, comments, and user profiles, would be permanently removed from the social network, as well as from any company storage. Reding highlighted how the seemingly innocuous fun of posting photos and messages on online social networks can backfire on individuals, for example, by jeopardizing job opportunities if viewed by a potential employer. In Germany, the Parliament (Bundestag) is already in the process of reviewing a draft bill that would explicitly prohibit employers from searching for information about job candidates on most online social networks; this development was discussed in Volume 1, Issue 3 of *Socially Aware*.

The other major EU legislative measure that would affect online social networks is the "privacy by default" rule. "Privacy settings often require considerable operational effort in order to be put in place," said Reding; a privacy by default rule would protect users by making built-in privacy mechanisms automatically "switched on" until users decide to change them. Privacy policies and settings on online social networks should be clear for the average user, said Reding, "easy to understand and easy to find." She explained that such a rule would also help prevent the surreptitious gathering of data "through, for example, software applications." Although this sort of rule would put users firmly in control of their personal data, it would have far-reaching consequences for the information economy, particularly data brokers and advertising networks that trade in information that may have been gathered without users' express consent.

Can You Shoot the Messenger?: Social Media Sites and Liability in the UK for Defamatory Third Party Content

In the United States, under Section 230 of the Communications Decency Act, website operators and other online service providers enjoy broad immunity from liability for defamatory comments posted by third parties. In other countries, however, the situation is less clear-cut. Social media services in particular have a global reach, and providers and users of such services need to pay careful attention to the heightened risks created by defamatory third party postings that are accessible outside of the United States—particularly in the UK, where even entities based outside the UK can be sued for defamation in UK courts by UK claimants (or by foreign claimants that have a reputation in the UK) if the defamatory content was viewed and/or downloaded in the UK. Below, we provide some background on UK defamation law; discuss strategies for preserving UK-specific defenses to defamation; and briefly explore the UK government's recently published draft bill intended to update defamation law in the UK.

Background: Although there is no general obligation in the UK for a website operator to screen or actively monitor third party content, a website operator may be liable in the UK for defamatory statements posted to its site by third parties, unless the operator can establish a defense under either section 1 of the Defamation Act 1996 or Regulation 19 of the E-Commerce Regulations 2002. (As used herein, "website operator" includes well-known Internet service providers, such as Google, and well-known social media sites, such as Facebook and Twitter, but also includes smaller-scale operators, such as individual bloggers and entities that host discussion boards.)

Under the Defamation Act 1996, a party has a defense to defamation if it can establish that it: (i) was not the author, editor, or publisher of the defamatory statement, (ii) took reasonable care in relation to its publication and (iii) did not know and had no reason to believe that it caused or contributed to the publication of the statement (the so-called "s1 defense"). (The s1 defense was first considered in *Godfrey v Demon Internet (1999)*, in which Demon Internet ("Demon") had received a complaint from Mr. Godfrey regarding a statement uploaded to a newsgroup hosted by Demon but took no action for ten days; the court held that Demon had published the material and could not avail itself of the s1 defense because it knew of the statement but chose not to remove it.) Under Regulation 19 of the E-Commerce Regulations, a provider of hosting services (including one who hosts websites, chat rooms, or blogs) can claim immunity with respect to third party defamatory statements if it is able to establish that it did not have knowledge of the defamation (the so-called "hosting defense"); however, such provider will lose this defense if, after becoming aware of the defamatory statement, it fails to act expeditiously to remove or disable

access to the defamatory statement.

Preserving defenses to defamation under UK law: Needless to say, each of the defenses described above may be crucial for an operator of a site or service that invites users to post third party or user-generated content, where the site is available in the UK. The following strategies may help an operator rely on the available defenses:

- *Delineate "acceptable" content:* The first line of defense is a robust set of end-user terms and conditions. A site operator should make clear in those terms and conditions what content is and is not acceptable to post.
- *Implement notice and take-down:* A site operator should create and implement a "notice and take-down" policy that permits the removal of allegedly defamatory postings. Unfortunately, as there is currently no statutory model for a notice and takedown procedure under UK law or any developed body of case law on the matter, it is unclear what constitutes "notice" to a website operator of defamatory content (and, therefore, what would trigger the operator's obligation to respond); how detailed or specific such notice needs to be; or even how quickly the operator needs to react in order to avail itself of applicable defenses. Each case would be considered on its merits. Accordingly, one of the safer approaches currently is for a website operator to indicate on its website how any such notice should be provided and what information should be contained in such notice, with any removal of content taking place within a reasonable time of receiving such notice. In addition, when formulating the terms describing its notice and takedown procedure, a website operator will need to ensure that those terms are compliant with applicable UK law (for example, if dealing with consumers, the Unfair Contract Terms in Consumer Contracts Regulations 1999 ("UCCR")). (In order to avoid its terms being found unfair under the UCCR and therefore invalid, the website operator will need to ensure that its right to remove content is not too widely drawn, but is subject to a reasonableness test—for example, that the right to remove content arises if removal is required in the operator's "reasonable opinion" or, having received notice of a complaint, the operator "reasonably believes" that the material is defamatory.)
- *Keep appropriate records:* Site operators ideally should maintain accurate, time-stamped records of complaints received and content removed, including what remedial actions were taken.
- *Avoid monitoring/moderation:* Site operators should carefully evaluate whether or not to carry out pre- or post-publication monitoring of content posted by third parties. In theory, active monitoring or moderation of content could limit the potential for defamatory statements to be posted. However, some operators may simply not have the resources to carry out effective monitoring or moderation, and moreover, monitoring or moderation could increase the risk that an operator will be considered an "editor" or "publisher" of the applicable content—which could lead to a loss of the s1 and hosting defenses (as highlighted in the case of *Kaschke v Gray & Hilton (2010)*). Accordingly, many operators simply choose not to carry out any monitoring or moderation, and instead rely solely on "notice and take-down."
- *Avoid exerting editorial control:* As noted above, website operators should be careful not to exert any form of editorial control over third party content, whether pre- or post-publication, as such editorial control could cause an operator to lose the benefit of the s1 and/or hosting defenses. Even minor amendments to spelling and grammar or promoting posted content to a more prominent position on a blog/site is likely to turn a website operator into an "editor" of the content and take the operator outside of the available defenses (see *Kaschke v Gray & Hilton (2010)*).

The future of UK defamation law: On March 15, 2011, in response to concerns regarding current deficiencies in the UK's defamation laws, the UK Ministry of Justice published a draft Defamation Bill for consultation that contains various proposed amendments to such laws. Those amendments would, among other things, replace the defense of "fair comment" with a new defense of "honest opinion"; impose a requirement for claimants to demonstrate substantial harm before they sue; make it tougher for overseas claimants to bring claims in UK courts that have little connection to the UK; and establish a "single publication" rule, meaning that repeat claims for libel would not be able to be made each time a publication is accessed on the Internet. For a copy of the draft bill as published by the UK Ministry of Justice, click here.

Unfortunately, the draft Defamation Bill does not currently include draft provisions specifically addressing responsibility for the publication of defamatory statements on the Internet. The UK government indicates that Internet defamation issues merit further consideration and, in the consultation questionnaire that accompanies the draft legislation, is seeking the public's views on how the law should be changed to give greater protection to secondary publishers such as ISPs and discussion forums in order to strike a fair balance between the interests of freedom of expression and the rights of individuals to protect their reputations. In part, the UK government is seeking feedback on whether difficulties have arisen from the current voluntary notice-and-takedown arrangements; whether or not a notice-and-takedown procedure should be prescribed statutorily to help website operators protect themselves from liability and preserve applicable defenses; and if so, what forms of notice and notice windows would be appropriate. The consultation period ends on June 10, 2011, after which the UK government will publish its responses and amend the bill before it is put before the UK Parliament in May 2012. We

will keep you informed of further key developments in this area.

Shaken, Not Stirred: Social Media and Alcohol Ads

Digital ads afford brands a varied set of powerful methods for leaving indelible impressions on consumers. Interactive "games," virtual product-themed environments, and brand-sponsored apps are just a few examples of how brands foster active viewership and, by extension, a more powerful identification. It follows that alcoholic beverages—products whose primary purpose are to foster sociability—have found social media to be a highly effective venue for consumer/brand interaction. Many alcohol makers have been quick to recognize these benefits; for example, Beam Global Spirits & Wine plans to increase its digital media expenditures to 35% of its marketing budget, compared to 6% only two years ago.

Although the form may vary from medium to medium, the message behind many alcohol ads often remains the same: brands want first and foremost to be associated with fun. Emphasizing *amusement* over the actual qualities of one's product is nothing new (Anheuser-Busch's Bud Bowl ads come quickly to mind). Social media, however, adds an extra dimension: alcoholic beverage companies can now more easily "sponsor" the consumption of their products. For instance, small wine companies can preserve brand integrity on a modest budget by using social media to distribute invitations to "exclusive" tastings. Some have even done away with the overhead of physical location-based tastings, opting instead for virtual tastings and tweetchats. Coupled with alcoholic beverage companies' active presences on services such as Twitter, smart event sponsorship (either virtual or real-life) can snowball into additional free advertising in the form of media coverage, re-tweets, and "trending" topics. And, of course, peer-generated word-of-mouth (the core of social media) may be the best advertising of all.

Still, advertisers should take care in structuring their branding efforts using social media services. Even though social media services collect vast quantities of user information, which arguably should make it easier for advertisers to target their ads in accordance with the law, reliable age verification may not currently be cost-appropriate for most marketing budgets and, what's more, social media's global reach can result in unintended consequences for marketers. And as we note below, the Federal Trade Commission ("FTC") is starting to take a fresh look at the alcoholic beverage industry's advertising practices, which may include a look at the industry's social media advertising practices as well.

When alcoholic beverage makers initially ported television advertisements (and advertising strategies) to the Internet, consumer groups and others alleged that many of these companies were using the new medium to evade generally accepted advertising standards and target minors. In 2007, Anheuser-Busch launched Bud.tv, an early entertainment portal designed to capitalize on the popularity of its YouTube-based Budweiser commercials; the site had been operating for less than a month when twenty-one state Attorneys General joined together to attack the site's age verification methods as ineffectual. Similarly, Diageo, the makers of drinks such as Smirnoff Ice, Bailey's, and Guinness, came under fire in 2008 for allegedly targeting the youth market through its own YouTube advertisements.

Alcoholic beverage companies have defended themselves against these allegations, arguing that their Internet ads meet the industry's self-imposed marketing standards. Currently, alcohol advertising is governed by a voluntary, self-regulatory regime led by three trade groups: the Distilled Spirits Council of the U.S. (DISCUS), the Beer Institute, and the Wine Institute. These groups typically classify a medium as "acceptable" or "unacceptable" for alcohol advertisements based on the age distribution of the particular medium's consumers. Reportedly, each of the Beer Institute's 2006 "Advertising and Marketing Code," DISCUS's 2010 "Code of Responsible Practices for Beverage Alcohol Advertising and Marketing," and the Wine Institute's 2005 "Code of Advertising Standards," deems a given medium to be acceptable for alcohol advertising where "at least 70 percent of the audience is reasonably expected to be above the legal purchase age." In defending Bud.tv, Anheuser-Busch has pointed to YouTube's usage statistics, which show at least 70% of the audience to be of legal drinking age.

On the other side of the equation, many popular ad services and social media platforms that serve ads have worked restrictions on alcohol advertisements into their respective terms of use. AOL, Google, and Facebook each have written policies restricting the marketing of alcoholic beverages on their respective services. AOL's ad policy largely maps to the industry's self-regulatory policies, and other services, such as YouTube, refer to local laws and standards. Several of these policies, as well as other means used by social media services to restrict the availability of alcohol ads, rely on some combination of age-based and geographic restrictions, whether enabled by the services themselves or by the advertisers where possible. Facebook's Statement of Rights and Responsibilities restricts the development and operation of third party applications containing alcohol-related content, prohibiting such activities "without appropriate age-based restrictions." Further, where a Facebook user's age or geographical location cannot be determined, an alcoholic beverage ad "cannot be displayed" to that user. Twitter requires more limited information from new users than other services—it does not require new users to supply age or geographic information—and therefore

does not rely on profile checks for age/geographic verification. Neither, of course, can its users; reportedly, some beer brands utilizing Twitter require users to direct message ("DM") the brand first, before being able to follow itsTwitter feeds.

The lack of clear solutions to these issues potentially impedes both social media services and the alcoholic beverage industry. Commentators note that Twitter, for instance, was initially reticent to offer its "promoted tweet" service to alcohol brands and that, although Twitter has since expanded the popular service to include more brands, including a select few in the alcohol industry, as of early February 2011, no alcoholic beverage companies had yet taken advantage of the service.

Of course, developments in this area have not gone unnoticed by the Federal Trade Commission (FTC). By and large, the FTC has relegated its role to offering advice on the industry's self-imposed advertising limitations, and one of the FTC's more recent efforts—a call to increase the generally-accepted demographic standard from its current 70% to 75%—has been largely ignored by the industry, according to *Advertising Age*. This situation may be changing, however, as the FTC has recently made clear its intention of scrutinizing the relationship between social media and alcohol more closely. The FTC announced on March 8, 2011 that it is beginning a study of the self-regulatory efforts of the alcoholic beverage industry, and is seeking comment on its proposed collection of data from alcoholic beverage companies, with topics to include "the status of third party review of complaints regarding compliance with voluntary advertising codes." Commentators suggest that one focus of the FTC is likely to be the alcohol industry's use of social media and social marketing, potentially including "information collection and credibility of age restrictions." If the FTC does take a more active role in this area, it will mark a shift from past practices. In a future issue of *Socially Aware*, we plan to explore how the tobacco industry has responded to issues similar to those outlined above.

The Rise (and Possible Demise?) of Copyright Trolls

Media companies and other large content providers regularly bring copyright infringement suits to prevent the unauthorized use of their content online. For example, the Associated Press recently threatened to take legal action to curb the unlicensed use of its content by bloggers and news aggregators. Beginning last year, however, social networking services and other user-content focused websites began to see a new trend in online copyright enforcement: so-called *copyright trolls*, entities that, much like the "patent trolls" (or "non-practicing entities") from which the term derives, focus on acquiring copyright rights not for purposes of publishing the copyrighted content, but for purposes of enforcement. Copyright trolls scour the Internet for unauthorized use of such content, and attempt to enforce their newly-acquired rights against the alleged infringers.

In the summer of 2010, Righthaven LLC began filing copyright infringement lawsuits against bloggers and website operators for reproducing on their blogs and websites portions of articles and images that Righthaven had recently purchased. Reportedly, the company then used the threat of protracted litigation, coupled with the potentially painful remedies for infringement that the Copyright Act affords (including statutory damages for willful infringement of up to $150,000 per instance), to force settlements. As of mid-April 2011, Righthaven has reportedly filed approximately 265 lawsuits, often against defendants described as "mom and pop" websites, public interest groups and other poorly funded entities. Two recent decisions, however, may cast doubt on the viability of Righthaven's infringement claims and the company's efforts, in the words of the Electronic Frontier Foundation ("EFF"), to turn "copyright litigation into a business model."

In an October 2010 district court case in Nevada, *Righthaven v. Realty One Group, Inc.*, the court granted defendant Realty Group One, Inc.'s motion to dismiss, ruling that the real estate firm's reprinting of eight of the thirty sentences from a *Las Vegas Review Journal* article without permission was a protected fair use. The court noted that the defendant only copied a small part of the factual portion of the copyrighted work and that the reproduction at issue was not likely to have an effect on the market for the article, two of the four factors typically considered under the Copyright Act's fair use doctrine. Although there is no bright-line rule under the Copyright Act for how much of a given work can be reproduced without running afoul of the fair use doctrine, the court's brief and unqualified dismissal of Righthaven's claim may call into question the continued viability of Righthaven's legal strategy (particularly with respect to alleged infringers who reproduce only a small portion of a given work) and may signal to defendants the possibility of successfully countering Righthaven's allegations. Indeed, soon after this decision was issued, Righthaven announced that it no longer planned to sue websites for posting brief excerpts of newspaper articles that it owned.

This April 2011, Righthaven suffered another loss, as more recently reported, in the matter of *Righthaven v. Center for Intercultural Organizing* ("CIO"). In this case, Righthaven sued an Oregon-based, not-for-profit immigrant rights organization in federal district court in Nevada for reprinting a full article from the *Las Vegas Review-Journal*. At a hearing held on March 18, 2011, the court announced it's intention to dismiss the lawsuit on the basis that Righthaven's legal arguments were unavailing and that CIO's use of the article was likely a protected fair use. In addition to reiterating several points raised by the court in the *Realty One Group* case, the *CIO* court took issue with the fact that Righthaven was assigned the subject work solely "to support a lawsuit," and stressed that the defendant's use was unlikely to impact the market for the work—*despite the fact that the article had been reprinted*

in full—because "[t]he market (served by the CIO) is not [plaintiff's] market." The court noted that the highly factual nature of the allegedly infringed work and the fact that the defendant was a not-for-profit entity were relevant to its reasoning, but also stressed that permitting the use of copyrights solely to support lawsuits would likely have a chilling effect on free speech, and does not advance the purposes of the Copyright Act to encourage and protect creativity. The *CIO* court reiterated this reasoning in it's subsequent April 11, 2011 order, in which it granted summary judgment in favor of *CIO* on fair use grounds. In its order, the court noted that, because Righthaven's only interest in the copyright was to bring suit, Righthaven could not claim the *Las Vegas Review Journal*'s market as its own and had failed to allege that a "market" exists for its copyright at all.

Statements made by both the *CIO* court and the *Realty One Group* court highlight another point that media commentators have found objectionable, namely, the putatively "predatory" nature in which Righthaven selects and pursues defendants. The *CIO* court noted, for example, that given that Righthaven never informed CIO of its alleged infringement or sent CIO any sort of "take-down" or similar notice, CIO had no opportunity to stop infringing before Righthaven filed suit. *Wired* reports that Righthaven appears to be targeting websites that have failed to comply with crucial copyright law formalities, such as the DMCA's obligation to designate an agent to receive notifications of claimed infringement, in order to avoid having to send take-down notices. Needless to say, as a practical matter, website owners and operators should be aware of, and comply with, the technical requirements of the DMCA's safe-harbor provisions in order to provide a measure of protection against claims such as those brought by Righthaven.

Righthaven actively continues to bring new claims. As recently as December 2010, the company partnered with the nation's second-biggest news chain, Denver-based MediaNews Group (which owns the *San Jose Mercury News* and *Denver Post,* among other news sources), and began filing copyright infringement suits on MediaNews' behalf. Still, considering the cases described above and the continued opposition to Righthaven's lawsuits by public interest groups, law professors, and others, Righthaven's strategy may be losing momentum. Additionally, several other suits are still being litigated and may provide further insights regarding Righthaven's claims. For example, in another Righthaven suit, the EFF has alleged that a content provider's assignments of copyrights to Righthaven, purporting to give Righthaven the standing to sue website operators, are "a sham designed solely to pursue litigation[.]" It may be, as one reporter puts it, that in continuing to file lawsuits, Righthaven has provided courts with an overdue opportunity to clarify the scope of fair use online and that "newspapers now have less—not more—protection from copyright infringers."

If you wish to subscribe to *Socially Aware*, please send an email to sociallyaware@mofo.com. To review earlier issues of *Socially Aware*, visit us at http://www.mofo.com/sociallyaware/.

About Morrison & Foerster

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, *Fortune* 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last seven years, we've been included on *The American Lawyer*'s A-List. *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger. This is MoFo.

Because of the generality of this newsletter, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. The views expressed herein shall not be attributed to Morrison & Foerster, its attorneys or its clients.

©2011 Morrison & Foerster LLP | mofo.com