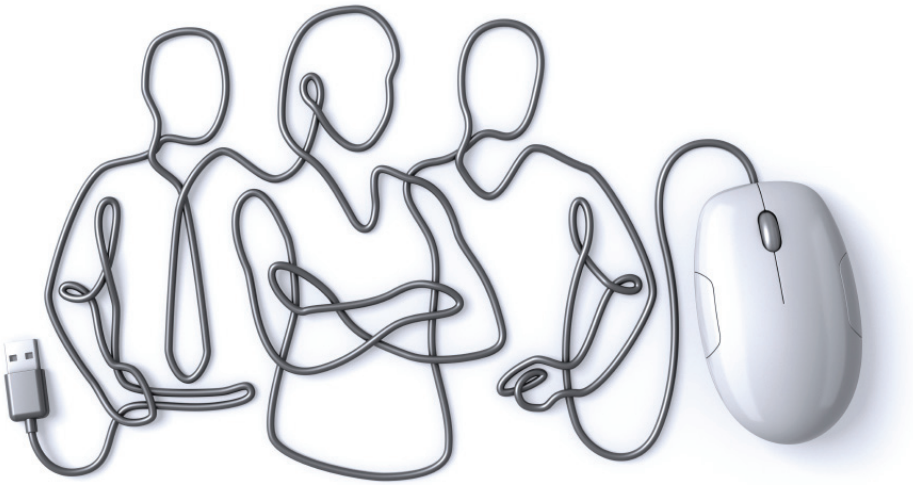
Morrison & Foerster Social Media Newsletter

Vol. 3, Issue 1 January 2012

Socially Aware:
The Social Media Law Update

2011 Best Law Firm Newsletter

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION



We welcome you to a special New Year's edition of *Socially Aware*, our Burton Award-winning guide to the law and business of social media. To kick off 2012, we provide our predictions for the coming year, and we take a nostalgic look back at the most popular topics on Facebook, Twitter and YouTube in 2011. We also compare the contest and sweepstakes rules of three major social media platforms; discuss the FTC's proposed order settling its claims against Facebook's privacy practices; review the emerging case law regarding the discovery of the identities of anonymous Internet users; highlight recent disclosures relating to Facebook's online tracking of Facebook.com visitors; provide an overview of FINRA's updated guidance to broker-dealer members on social media usage; and take a close look at a recent court decision applying intellectual property laws to user-created virtual objects. And we conclude with *Status Updates*, our round-up of social media news items.

On a related note, we are delighted to announce the launch of our new Socially Aware blog at www.sociallyawareblog.com. You can also follow us on Twitter @MoFoSocMedia.

IN THIS ISSUE

EDITORS

John Delaney
Gabriel Meister
Aaron Rubin

CONTRIBUTORS

Seth Graham
David Kiferbaum
Julie O'Neill
Karin Retzer
Hashem Sabbagh
Sunni Yuen
Daniel Zlatnik

Running Contests and Sweepstakes on Facebook, Google+ and Twitter: How the Rules Stack Up

Over the past two years, *Socially Aware* has revisited Facebook's Promotions Guidelines from time to time — even as recently as August 2011 — to help keep our readers up-to-date on how popular social media platforms seek to regulate contests, sweepstakes and other promotions.

Online promotions are as popular as ever, and given that two-thirds of American adults now use some type of social media platform, we decided to take a broader, comparative look at the promotions guidelines of three major social networks — Facebook, Google+ and Twitter — to give our readers a sense of how these guidelines stack up.

A social network's terms and conditions governing promotions are typically a mix of rules, restrictions and best-practices suggestions that can be difficult to navigate. Equally tough to digest are the dozens of "how to" websites that purport to instruct social media users how to conduct successful (and legal) promotions online, and the numerous companion sites that advertise social media promotions to anyone who wishes to join. What's more, social media services' promotions policies are updated and amended frequently, as we have noted previously, and they typically incorporate or are incorporated into other, far more general rules and restrictions that both protect the respective service providers and give those providers considerable latitude in accepting, rejecting, suspending or terminating promotions on their platforms.

Here's a quick look at where Facebook's, Google+'s and Twitter's promotions guidelines stand today:

1. Google+. Let's start with Google+, the newest social network on our list. Google+ recently published its policies for contests and promotions. Simply put, Google+ users are not permitted to run contests, sweepstakes, offers, coupons or other such promotions directly on their Google+ Pages; however, users *are* permitted to post links on their Google+ Pages to such users' promotions on other sites, as long as they agree to be solely responsible for such promotions and for compliance with all applicable laws, rules and regulations. (In a sense, this approach mirrors Facebook's rule, discussed in our August 2011 issue, on communicating about promotions: "If you use Facebook to communicate about . . . a promotion, you are *responsible for* the lawful operation of that promotion.") Some have noted that Google+'s restrictive promotions policies are somewhat counterintuitive in light of Google+'s recent launch of "Brand Pages," which finally enable brands, products, companies, businesses, places, groups, and everyone else to establish branded presences on the fledgling service.

User promotions that are linked from users' Google+ Pages are required to adhere to a variety of other Google+ terms and conditions, including the Google+ Pages Additional Terms of Service. Those terms incorporate by reference even more Google+ terms and conditions, such as the Google+ User Content and Conduct Policy. Google retains the right both to remove a user's "Promotion content" from the user's Google+ Page for any reason and to block or remove Pages that violate Google+'s Pages terms (and even, in the case of repeat violations of the Pages terms, to suspend the user's Google+ account).

One other interesting point: For now, according to the Google+ Pages Additional Terms of Service, "[e]xcept as otherwise required by the Google+ Pages Terms, you may not include terms, conditions or non-Google provided technical restrictions on Google+ Pages." This implies that, even though a user is permitted to link to the user's promotion from his or her Google+ Page, the user is *not* permitted to include on the Page any "terms" or "conditions" governing the promotion — let alone the promotion's "Official Rules."

Simply put, Google+ users are not permitted to run contests, sweepstakes, offers, coupons or other such promotions directly on their Google+ Pages.

2. Twitter. In contrast to Google+'s prohibitive policies, Twitter specifically permits users to operate promotions on its platform. In fact, Twitter's Guidelines for Contests on Twitter (the "Twitter Guidelines," which despite their name, govern both contests and sweepstakes) take a different approach from other platforms' promotions terms, as they read more like a set of suggestions that promotions operators are *encouraged* to follow in order to generally enhance the Twitter user experience and to steer entrants clear of violating other Twitter rules. (Unlike the promotions guidelines for Google+ and Facebook, the Twitter Guidelines do not distinguish between promotions "run on" Twitter and those merely advertised on or promoted using Twitter; the guidelines simply govern any contests and sweepstakes "on Twitter," for example, offering prizes for Tweeting updates, following a particular user or posting updates with a specific hashtag.)

As an example, the Twitter Guidelines admonish users to discourage the creation of multiple accounts (which could lead to account suspension under

"The Twitter Rules") by "be[ing] sure to" impose a rule that users will be ineligible if they create multiple accounts to enter a promotion more than once. The Twitter Guidelines also note that users "might want to set a clear contest rule" that multiple entries from a given entrant in a single day will not be accepted, in order to help discourage posting of the same Tweet repeatedly (e.g., "whoever re-Tweets the most wins").

3. Facebook. While Google+'s promotions guidelines flatly prohibit onsite promotions and instead focus on how users can *communicate* about their offsite promotions, and Twitter's guidelines do not distinguish clearly between operating and communicating about promotions on Twitter, Facebook's Promotions Guidelines squarely address both *communicating about* and *operating* promotions on Facebook.

Facebook's Promotions Guidelines get into plenty of detail on how promotion operators can and cannot use Facebook and its many features to operate promotions. A few highlights:

- *Promotions operated on Facebook must be administered using Apps on Facebook*, Facebook's development tools for app builders, both to ensure interoperability with Facebook's platform and to enable Facebook to advertise to users of the app.
- *Promotions operators are required to make certain mandatory disclosures*, including (i) a complete release of Facebook by each entrant, (ii) an acknowledgement that the promotion is not sponsored, endorsed or administered by Facebook, and (iii) that the entrant is providing information to the promotions operator only and not to Facebook. (Neither Google+ nor Twitter requires disclosures such as these, although Google+'s promotions terms include broad language releasing Google from liability for users' promotions and requiring users to indemnify Google from claims and losses arising from such promotions, and Twitter's general terms simply disclaim any liability for Twitter's use of content provided by Twitter users.)
- *Facebook features and functionality cannot be used* (i) as a way to register for or enter a promotion (e.g., "Liking" a Facebook Page cannot constitute an entry in a promotion), (ii) as a prerequisite to participating in a promotion (although promotion operators are permitted to require users to Like a Page, check into a Place, or connect to the operator's page in order to enter a promotion), (iii) as a promotion voting mechanism, or (iv) to notify promotion winners (e.g., through messages, chat, or posts on profiles or pages). This is an interesting contrast to the Twitter Guidelines, which imply that Twitter is comfortable with the use of a wide range of Twitter features in connection with Twitter-based promotions.

2011: TOP STATUS UPDATES

1. Osama bin Laden's Death
2. Green Bay Packers' Super Bowl Victory
3. Casey Anthony "Not Guilty" Verdict
4. Charlie Sheen
5. Steve Job's Death
6. The Royal Wedding
7. Amy Winehouse's Death
8. Call of Duty: Modern Warfare 3
9. Libya Military Operations Commence
10. Hurricane Irene

Note: Shows Status Update Mentions Ranked by Growth (2011 vs 2010)

Source: http://www.allfacebook.com/facebook-status-updates-2011-2011-12

Conclusions. The promotions guidelines promulgated by Facebook, Google and Twitter reveal a few common threads. Each service seems to be concerned with protecting its community members, for example, by restricting the creation of false accounts, by prohibiting the publication of misleading or false information or by limiting the collection and use of personal information by promotions operators for purposes other than the promotion itself. Similarly, each service's guidelines require promotion operators to take certain actions to ensure that their promotions

do not interfere with, and are otherwise compatible with, the general functioning of the service. Finally, each provider has put measures in place to shield itself from the legal complications arising from operating or communicating about promotions on its service — in at least one case (Google+), by prohibiting the operation of promotions outright.

Moreover, keep in mind that a social media site's promotions guidelines are only part — typically, a very *small* part — of the universe of terms and conditions that bind promotions operators. Each service described in this article requires compliance with various other site-specific policies, terms and conditions, which often further restrict how promotions can be run or advertised. Google+'s promotions guidelines link to three other Google+ policies, each of which links to several other policies that impose additional restrictions, for example, the Google+ Pages Additional Terms of Service's prohibition on posting content that violates third-party rights or content that is considered inappropriate under yet another policy, the Google+ User Content and Conduct Policy. Similarly, Twitter requires all promotions operators to comply with The Twitter Rules and Twitter's search best practices before commencing a promotion, and Facebook supplements its Promotions Guidelines by requiring promoters to comply with Facebook's Statement of Rights and Responsibilities (which, as we have noted previously, incorporate many other Facebook policies), its Ad Guidelines, and its Platform Policies. And bear in mind that all of these policies, rules and guidelines change over time.

The complexity of social media services' various promotions guidelines, rules and best practices means that any would-be promotions operator needs to carefully review — and monitor over time — each service's terms, particularly when a promotion is designed to leverage multiple social media services simultaneously. First-time social media promotions operators in particular may want to seek legal guidance, both in understanding each target service's terms and in helping to craft a set of "Official Rules" that can help the operator manage risk and maximize the chances of running a successful social media promotion.

Proposed Facebook Settlement Underscores the FTC's Privacy Priorities

On November 29, 2011, the Federal Trade Commission ("FTC") announced a proposed order against Facebook that builds upon both the FTC's recommendations from its 2010 draft privacy report and precedents set in the order that it recently imposed on Google. Any business that collects personal information from consumers should pay close attention to this action because it makes clear that:

- ***The FTC will continue to remain vigilant in holding companies to their privacy-related promises to consumers.*** The FTC will pay particular attention when those promises involve consumers' choices regarding their personal information, and it will continue to look for and prosecute companies who have certified their compliance with the U.S./EU Safe Harbor (allowing personal information collected in the EU to be transferred to the US) yet fail to abide by the principles underlying the Safe Harbor;
- ***The FTC will continue to require opt-in consent for material changes to a company's privacy practices.*** This is not a new development, but it is worth repeating that the FTC has not backed away from its assertion that, when a company changes its privacy practices in a material way, it must obtain consumers' opt-in consent to those changes before applying them retroactively (i.e., to information already collected);
- ***The FTC has a robust new template for privacy orders.*** The FTC will continue to impose onerous injunctive relief on companies that do not abide by their own privacy promises, including the obligation — even where there has been no alleged data breach — to obtain an independent privacy audit every other year for 20 years; and
- ***The FTC will continue to require companies subject to a privacy order to implement and maintain a comprehensive "privacy by design" program and, in fact, may begin to expect this from all companies.*** In its 2010 draft privacy report, the FTC proposed that businesses make privacy and data security a routine consideration by adopting a "privacy by design" approach. The report has not yet been finalized, but that has not stopped the FTC from moving this proposal closer toward becoming a legal requirement by way of its enforcement actions against Google and Facebook (the FTC often expresses its "expectations" of industry through settlement agreements). We take the inclusion of a "privacy by design" requirement in both orders to mean that the FTC thinks that all businesses should adopt such procedures and that, eventually, the FTC is likely to view a failure to adopt such procedures as deceptive or unfair, in violation of the FTC Act.

The proposed order would settle charges that a variety of Facebook's information practices were deceptive or unfair. Highlights of the complaint and proposed order are summarized below. The proposed order was open for public comment until December 30, 2011; that period having closed, the FTC will now

determine whether to make its order final or to modify its requirements.

The FTC's Complaint

The FTC's complaint against Facebook contains eight counts, each of which underscores the theme repeated in the FTC's privacy enforcement actions over the years: Businesses must comply with the privacy-related promises that they make to their customers. Here, the FTC alleged that Facebook failed to comply with promises made to its users in a variety of contexts over time. Specifically:

- **Facebook's privacy settings: Access to personal information.** Facebook promised its users that, through the choices that they made in their Profile Privacy Pages, they could limit the categories of people who could access their personal information. According to the FTC, however, users' choices were meaningless because Facebook permitted third-party applications used by a user's Facebook friends to access the user's personal information — including marital status, birthday, town, schools, jobs, photos, and videos — regardless of the privacy settings chosen by the user. The FTC has therefore alleged that the company's representations were deceptive.

- **Facebook's privacy settings: Overriding user choice.** Two counts in the FTC's complaint address privacy policy changes that Facebook made in December 2009 — changes that Facebook claimed would not only give users more control over their personal information but also allow them to keep their existing privacy settings. According to the FTC, contrary to those promises, some information designated by users as private (such as a friend list) was actually made public under the new policy. The FTC has charged that this was deceptive because Facebook overrode users' existing privacy choices without adequate disclosure.

Specifically, the order would enjoin Facebook from express and implied misrepresentations about how it maintains the privacy or security of users' information.

The FTC has further charged that the change constituted an unfair practice because Facebook retroactively applied material changes to personal information it had already collected from users without first obtaining their consent. In the FTC's view, the practice met the standard for unfairness because it "has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers."

- **Scope of applications' access to user information.** The FTC has alleged that, for more than three years from the debut of applications on the Facebook platform, Facebook deceived its users about the scope of the profile information accessible to apps. Specifically, Facebook told users that an app would have access to only the information "that it requires to work." The FTC has charged that this promise was deceptive because, in many instances, Facebook gave apps unrestricted access to user profile information, including information that such apps often did not need to operate.

- **Advertisers' receipt of user information.** According to the FTC's complaint, Facebook represented to users numerous times that it would not share their information with advertisers without the users' consent. For instance, in its Statement of Rights and Responsibilities, Facebook promised: *"We don't share your information with advertisers unless you tell us to. . . Any assertion to the contrary is false. Period . . . we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads."* The FTC has alleged that this representation and others like it were deceptive because, from at least September 2008 until the end of May 2010, Facebook's site was designed and operated such that the User ID of a user who clicked on an advertisement was, in many cases, shared with the advertiser.

- **Facebook's "Verified Apps" program.** Facebook promised its users that, under its "Verified App" program, Facebook reviewed apps so as to "offer extra assurances to help users identify applications they can trust — applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with [Facebook] policies." According to the FTC, however, because Facebook did not take any steps to verify an app in any of these ways, its promise was deceptive.

- **Photo and video deletion.** Facebook told users that, when they deactivated or deleted their accounts, their photos and videos would be inaccessible to others. The FTC has alleged, however, that Facebook continued to make available the photos and videos of both deactivated and deleted accounts to third parties, and, accordingly, the company's promises were deceptive.

- **Compliance with the U.S.-EU Safe Harbor Framework.** The FTC has alleged that Facebook misrepresented its compliance with its Safe Harbor certification because — as described above — it failed to give its users notice and choice before using their information for a

purpose different from that for which it was collected, in violation of the "Notice" and "Choice" principles required of Safe Harbor certified companies. Because Facebook's Safe Harbor certification represented to consumers that Facebook was compliant with the principles, the FTC has charged that its failure to comply with them was unfair or deceptive.

The Proposed Settlement Agreement

No Privacy or Security Misrepresentations. Like all FTC orders settling charges of deception, the proposed order would prohibit Facebook from future misrepresentations. Specifically, the order would enjoin Facebook from express and implied misrepresentations about how it maintains the privacy or security of users' information, including: (1) the extent to which a user can control the privacy of his or her information; (2) the extent to which Facebook makes user information available to third parties; and (3) the extent to which Facebook makes information accessible to third parties after a user has terminated his or her account.

Opt-In Consent for New Disclosures. The proposed settlement agreement would require Facebook to obtain users' opt-in consent before sharing their information with a third party in a way that materially exceeds the restrictions imposed by the users' privacy settings. This obligation ratifies a requirement that the FTC first imposed against Gateway Learning in 2004 and which it has repeated numerous times since then: A company that makes a material change to its privacy practice must obtain affected individuals' opt-in consent to that change before applying it retroactively (i.e., to information already collected). The proposed order specifies the way in which Facebook must obtain such consent. It must: (1) clearly and conspicuously disclose to the user, separate and apart from any privacy policy or similar document, (a) the categories of information that will be disclosed, (b) the identity or categories of the recipients, and (c) the fact that such sharing exceeds

2011: MOST EVENTS

1. 12/9/11: Japanese television screens the 1986 animated film Castle in the Sky (25,088 Tweets/second)
2. 8/28/11: Beyoncé reveals her pregnancy at the MTV Video Music Awards (8,868 Tweets/second)
3. 9/20/11: Users tweet to raise awareness in advance of Troy Davis's execution (7,671 Tweets/second)
4. 7/17/11: Japan beats the U.S. at the Women's World Cup (7,196 Tweets/second)
5. 7/17/11: Brazil is eliminated from the Copa America soccer tournament (7,166 Tweets/second)
6. 8/25/11: Steve Jobs resigns as CEO of Apple (7,064 Tweets/second)
7. 1/1/11: Midnight, New Years Eve in Japan (6,939 Tweets/second)
8. 6//27/11: BET Awards airs featuring a confused Viewers Choice Award (6,436 Tweets/second)
9. 5/28/11: The UEFA Champions League soccer tournament's final match airs (6,303 Tweets/second)
10. 10/5/11: Apple founder and CEO Steve Jobs dies (6,049 Tweets/second)

Source: http://www.mediabistro.com/alltwitter/twitters-tweets-per-second-record-breakers-of-2011-infochart_b17210

the restrictions imposed by the user's privacy settings; and (2) obtain the user's affirmative express consent to the disclosure.

Deletion of "Deleted" Content. The proposed settlement would require Facebook to implement procedures reasonably designed to ensure that the information of a user who has deleted his or her information or deleted or terminated his or her account is not accessible by any third party.

Privacy by Design. Like the FTC's order against Google, the proposed Facebook order includes a "privacy by design" provision that would require Facebook to implement and maintain a comprehensive privacy program that (1) addresses the privacy risks related to the development and management of both new and existing products and services and (2) protects the privacy of user information. Specifically, Facebook would have to:

- designate one or more responsible employees;
- identify reasonably foreseeable material risks that could result in the unauthorized collection, use or disclosure of user information;
- design and implement reasonable controls and procedures to address identified risks and regularly test them;
- develop and implement reasonable steps to select service providers that will adequately protect user privacy and contractually require them to maintain appropriate protections; and
- evaluate and adjust the privacy program in light of the testing required by it, any material change to Facebook's operations, or any other circumstances that may have a material impact on the program's effectiveness.

In its 2010 draft privacy report, the FTC proposed that businesses make privacy and data security a routine consideration by adopting a privacy by design approach. Although it has not yet finalized the report, the FTC has moved this proposal closer to becoming a legal requirement through both its proposed order and its recent order against Google. The FTC often expresses its expectations of industry through a settlement agreement. For this reason, we take the inclusion of a privacy by design requirement in both orders to mean that the FTC thinks that all businesses should adopt such procedures and that, eventually, the FTC is likely to view a failure to have them as deceptive and/or unfair, in violation of the FTC Act.

Biannual Audits for 20 Years. The proposed settlement agreement would require Facebook to obtain an independent privacy audit every other year for 20 years. In light of the fact that this is the second time that the FTC has imposed such relief this year (after the Google matter), we expect that the 20-year audit requirement along with the privacy by design provision, will become a staple of FTC privacy settlements.

Safe Harbor Provisions. The proposed settlement marks the second time that the FTC has held a company accountable for its alleged failure to comply with substantive privacy provisions of the US/EU Safe Harbor framework. (The first was in the Google action.) The charges serve as an important reminder that Safe Harbor certification constitutes a representation to consumers that, if false, is actionable. The proposed order would bar Facebook from misrepresenting its compliance with the Safe Harbor or any other privacy or security compliance program.

Key Take Aways

The FTC's complaint and proposed order against Facebook are noteworthy because they reinforce the precedents that the FTC set in its action against Google, thereby sending the following unmistakable signals to the market:

- The FTC will continue to hold companies to their privacy promises and apply strong injunctive relief where it finds that the promises are false;
- The FTC continues to believe that a company must obtain affected consumers' affirmative consent to new privacy practices applied retroactively;
- The FTC will continue to look for and prosecute companies' failures to abide by the principles underlying their US/EU Safe Harbor certifications;
- The FTC has a new template for privacy settlement agreements — one that requires a privacy by design approach to business, as well as independent biannual audits for 20 years; and
- The FTC is beginning to consider privacy by design as a requirement under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices.

Standard for Discovery of Anonymous Internet Users' Identities Remains in Flux

Plenty of press attention has been given to social media sites' views on whether their users can use "handles" or pseudonyms instead of their real names. But much of the Internet's social conversation remains dependent upon that dot-com staple, the anonymous message board. In the recent case of *Varrenti v. Gannett Co., Inc.*, a New York trial court had an opportunity to opine on the standard for compelling an online service provider (OSP) to disclose the identities of anonymous Internet posters in view of competing First Amendment considerations. However, the court punted on that issue, instead basing its decision on the far narrower question of whether plaintiffs stated a prima facie cause of action against the anonymous defendants — and leaving the standard

for discovery of anonymous Internet users' real identities unsettled in New York, just as it is nationwide.

A variety of tests for compelling the disclosure of the identity of an anonymous Internet user have emerged over the past decade. One approach is the five-factor balancing test established by a New York federal court in *Sony Music Entertainment Inc. v. Does 1-40*. Under the *Sony Music* test, a court is required to weigh the following five factors in order to assess the need to disclose an anonymous Internet user's identity:

- Is there a concrete showing of a prima facie claim of actionable harm?
- Is the discovery request sufficiently specific to lead to identifying information?
- Is there an absence of alternative means to obtain the subpoenaed information?
- Is there a central need for the subpoenaed information to advance the claim?
- Does the anonymous Internet user have a reasonable expectation of privacy?

An OSP's terms of service agreement can play into the fifth prong of the *Sony Music* test. In *Sony Music*, for example, the OSP's terms of service specifically reserved the right to disclose any information necessary to satisfy any law. Because the same terms also expressly prohibited users from transmitting material in violation of copyright law, the court found that the anonymous defendants had little expectation of privacy when using the service to download and distribute over peer-to-peer networks, sound recordings owned by third parties without permission of the copyright holders. Such a limited expectation of privacy, in conjunction with the plaintiff's strong prima facie claim of copyright infringement and the plaintiff's demonstrated need for the identifying information to advance its claim, outweighed any limited First Amendment protections that the service users might otherwise have.

Another test for whether the disclosure of an anonymous Internet user's identity can be compelled, is the four-factor test invoked by the Appellate Division of the New Jersey Superior Court in *Dendrite International, Inc. v. Doe No. 3*. In the lower court, Dendrite had sought to discover the identity of an anonymous poster on a Yahoo! Internet message board devoted to a discussion of Dendrite's stock performance. Dendrite alleged that the poster defamed the company and misappropriated trade secrets by making false statements about Dendrite having changed its revenue recognition policy, Dendrite's contracts being structured to defer income and Dendrite's lack of competitiveness, as well as by alleging that Dendrite's president was secretly and unsuccessfully "shopping" the company. The lower court judge found that the plaintiff was not entitled to discovery of the anonymous poster's identity because it had failed to show harm caused by the anonymous postings — a required element for stating a prima facie case of defamation.

A variety of tests for compelling the disclosure of the identity of an anonymous Internet user have emerged over the past decade.

On review, the Appellate Division adopted, with modifications, a four-factor test that had been applied by the federal district court in the Northern District of California in *Columbia Insurance Company v. Seescandy.com*. Under this test, a trial court is permitted to order the disclosure of an anonymous Internet user's identity if:

- The plaintiff makes efforts to notify the user that he or she is the subject of a subpoena, and affords the user a reasonable opportunity to file and serve opposition;
- The plaintiff identifies and sets forth the exact statements purportedly made by the anonymous user that allegedly constitute actionable speech;
- The plaintiff has asserted a prima facie cause of action against the defendant and produced sufficient evidence to support each element of the action; and
- The strength of the prima facie case presented, and the need for the disclosure of the defendant's identity, outweigh his or her First Amendment right of anonymous free speech.

The fourth prong of this *Dendrite* test is intended to be a "flexible, non-technical, fact-sensitive mechanism" that gives courts ample discretion to evaluate whether disclosure of the anonymous user's identity is necessary. Therefore, even though the lower court judge in *Dendrite* may have taken a stricter approach than normal to the "harm" element of the test (particularly when applying motion-to-dismiss standards), the Appellate Division determined that the judge's analysis of the claim was still consistent with that element of the test — and after determining that the record supported the lower court's finding that there was no nexus between the anonymous postings and fluctuations in Dendrite's stock prices, it affirmed the finding and refused to permit discovery of the anonymous poster's identity.

At least one court has found that the nature of the speech involved should be the driving force in selecting the test for discovering the identity of an anonymous Internet user. The Ninth Circuit has held that a stricter test for unmasking "John Doe" Internet publishers is appropriate when the speech at issue is non-commercial.

(continued on page 10)

Editors' Predictions for 2012

To ring in the New Year, the *Socially Aware* editors provide their predictions regarding social media law and business developments in the coming year (please keep in mind that, if we were good at this prediction thing, we wouldn't be practicing law for a living) . . .

Watch for an explosion of employment law disputes involving social media in 2012. It's coming. Get ready. You heard it here first.

We're going out on a limb here, but we believe that the Second Circuit may reverse and remand the lower court's decision in the widely-followed *Viacom v. YouTube* litigation, potentially creating turbulence for online companies that rely on user-generated content to attract traffic and boost revenues. Although the case raises some of the most important copyright issues of the digital era, the lower court's decision, favoring YouTube, did not dig into the details and nuances of the parties' respective arguments, and our sense is that the Second Circuit ultimately reverse that decision and send the case back to the lower court for further proceedings.

With the rise of social media platforms, we are seeing more and more companies — even Fortune 500 companies — entering into extremely one-sided "clickwrap" agreements with platform providers. Although clickwrap agreements are generally enforceable under U.S. law, we expect to see more challenges on public policy and other grounds to particular provisions in these agreements.

Speaking of clickwraps, we often comment on how social media platforms' terms of service (TOS) are typically long and intricate, branching off into various rules, policies, guidelines and "best practices" that change over time (and not necessarily all at the same time!). As business users invest more and more time and money in creating and cultivating their social media presences, and as consumers increasingly turn to social media as *the* way to interact with their favorite brands, we anticipate a resurgence of interest in what these TOS say… not just what they say today, but what they said last week, last month and last year. We foresee more services adopting Twitter's practice of maintaining an archive of earlier TOS versions, and perhaps even the institution of a well-stocked third-party clearinghouse, along the lines of TOSback.org, dedicated to tracking social media TOS changes over time.

Even with Facebook's recent settlement with the FTC in connection with Facebook's data collection practices, we anticipate still further privacy law headaches for social media companies in the coming year. Global privacy laws get tougher and more burdensome each year, and yet many social media providers, anxious to justify astronomical valuations, are undoubtedly feeling pressure to make more aggressive use of the personal information that they have collected from their customers. Watch for the first skirmishes in 2012 to be initiated by European regulators.

Online behavioral advertising is a subject that attracts strong bipartisan opposition, even in the current bitterly divided Congress. Watch for 2011's call for greater regulation of OBA to grow louder over the coming year, resulting in new legislation or regulations.

We will see even the largest, most conservative Fortune 500 companies adopting internal, company-wide social media platforms of the type offered by Jive, NewsGator and SocialText. And, in 2013 and beyond, we'll be seeing a new generation of privacy, employment, defamation and other legal claims arising out of these enterprise social platforms.

We will likely continue to see courts struggle with the limits of the safe harbors provided by Section 230 of the Communications Decency Act. Ever since the landmark 1997 case *Zeran v. America Online*, courts have fairly consistently held that Section 230 provides online service providers broad immunity for defamatory or otherwise actionable information posted by users. But we have also seen courts occasionally impose some limits on the scope of Section 230 -- e.g., in the 2008 case *Fair Housing Council v. Roommates.com* and the more recent *Hill v. StubHub* case. And other courts, such as the California Supreme Court in *Barrett v. Rosenthal*, have expressed discomfort with the broad sweep of Section 230 even while upholding it. Watch for more Section 230 cases in 2012 as courts continue to explore the outer boundaries of this critically important but controversial statute.

You don't need a crystal ball to see that mobile apps will continue to generate much of the growth in social network use and Internet use in general in 2012. Perhaps more interesting is the question of what form those apps will take and where users will get them. Various app stores and marketplaces, large and small, will continue to offer consumers many choices to shop for apps for different mobile platforms. And the emergence of HTML5-based apps as an alternative to native apps adds another dimension to the issue. We will likely see continued volatility in this area in 2012, but, if we were going to make a prediction — and that's what we're doing here, right? — our money is on HTML5-based apps to start taking market share from native apps in the coming year.

As the major global social media platforms vie for local eyeballs, we foresee more announcements like Twitter's recently-reported arrangement with Mixi, Japan's long-time favorite social media platform, to collaborate on new products and services. Partnerships like this, coupled with geographic expansion (Twitter opened an office in Tokyo in early 2011), could help the leading U.S. social media providers to establish brand recognition and ultimately market share in countries that are still ruled by home-grown incumbents.

(continued from page 8)

Under this test, originally established by the Delaware Supreme Court in *Doe v. Cahill*, a plaintiff may discover an anonymous speaker's identity by both giving or attempting to give notice to the speaker, and presenting a *prima facie* case that can survive a hypothetical motion for summary judgment. As reported in our August 2010 issue, the trial court in *Quixtar, Inc. v. Signature Management TEAM, LLC*, used this test to order the disclosure of the identities of anonymous speakers who had made allegedly false and disparaging statements about the plaintiff company on third-party blogs and in online videos. On appeal, the Ninth Circuit found that the district court's application of the *Cahill* test was not appropriate because the speech involved related to a non-compete provision in a contract, which was not express political speech entitled to greater protection. However, because the trial court's decision to apply the *Cahill* test did not constitute clear error, the Ninth Circuit nonetheless refused to vacate the trial court's order. It is unclear whether courts in other jurisdictions have adopted the approach of choosing a test based on whether the speech at issue is commercial or non-commercial.

The recent *Varrenti* decision reminds us that the assertion of a *prima facie* cause of action remains a key factor in determining whether the identities of anonymous Internet users are discoverable, no matter which test reigns. In *Varrenti*, members of the Village of Brockport Police Department brought a defamation action against the *Democrat & Chronicle*, a local newspaper publisher in Rochester, New York, and four Internet users who posted anonymous comments on the newspaper's website about the plaintiffs' competence, integrity and actions. The plaintiffs argued that the *Sony Music* test should apply, while the defendant argued that the *Dendrite* test should apply. The New York Supreme Court elected not to address the issue of which test applied, instead focusing on the common factor from both tests — that is, whether the plaintiffs had stated a *prima facie* cause of action for defamation. Because the tone and objective of the anonymous statements were critical of the plaintiffs and the comments were published in a web forum that invited newsreaders to share opinions, the court found as a threshold matter that the comments were protected expression that could not form the basis of a defamation claim, and that, therefore, no *prima facie* case had been stated.

In basing its decision solely on the context in which the comments were made, the *Varrenti* court avoided addressing other test factors, bringing no further clarity on which standard for discovering the identity of anonymous Internet users should apply. Until the various standards for discovery of anonymous Internet users' identity converge, then, the question of whether an OSP can be compelled to disclose an Internet user's identity rests largely on the plaintiff's ability to state a *prima facie* claim of actionable harm — worth keeping in mind for companies pursuing a claim against a user of a message board or other social media service.

Tracking the Trackers: Social Media Companies Face Pressure for Tracking Users' Browsing Habits

Facebook is facing renewed scrutiny following efforts to explain its data collection practices, which include tracking where and when members and non-members are browsing after they visit a Facebook page.

At the end of 2011, USA Today reported on how Facebook tracks user browsing habits, following in-depth interviews with senior Facebook engineers and spokespersons. According to those interviewed, any Facebook user who visits a Facebook page receives a "browser cookie" with a unique alphanumeric identifier; this cookie is then used by Facebook to track and create a time-stamped record of every visit by that user to any other website that utilizes a Facebook plug-in (such as "like" buttons), even if the user is logged out or not a member of Facebook. When a user is logged in to Facebook, an additional "session cookie" is activated, allowing Facebook to collect specific profile and system information (such as the user's email address and list of friends), user preferences and a time-stamped record of websites visited by the user that contain Facebook plug-ins. While Facebook only receives a user's personal information alongside his or her browsing history when the user is logged in to the Facebook service, users frequently remain logged in for long periods of time (merely closing a browser window or tab often is insufficient to end a session—rather, a user must affirmatively select the "log out" option made available by Facebook).

According to Facebook, this tracking information is used to boost security and to "enhance user experience" but *not*

In Belgium, Google has agreed to operate an online opt-out service through which individuals can ask for their entire image to be blurred if they still consider themselves to be recognizable on StreetView, and can request that images of their real property or other assets be blurred as well.

to target ads to Facebook users. Additionally, Facebook claims that it deletes tracking information that is more than 90 days old. However, with Facebook reportedly gearing up for a IPO in 2012, users and critics are concerned that the pressures of the public market will result in more aggressive leveraging of users' browsing habits and associated data in an effort to maximize profits.

Meanwhile, courts have been actively adjudicating claims against online service providers that may be using (or abusing) user information. In November 2011, a LinkedIn user's class action lawsuit against LinkedIn for allegedly disclosing the user's browsing history to third parties was dismissed for lack of constitutional standing to sue. The plaintiff in the Northern District of California case, *Low v. LinkedIn Corp.*, claimed that he was "embarrassed and humiliated" by LinkedIn's alleged disclosures of "valuable personal property" (his browsing history and related personal information). The court found that the plaintiff's allegations lacked particularity in failing to explain what personal information was disclosed to third parties, how it was disclosed, and to what extent it actually resulted in economic injury. Failure to allege "injury-in-fact" resulted in a successful motion to dismiss for LinkedIn; however, the court has provided the plaintiff with an opportunity to amend his complaint to allege "particularized" examples of his actual injury.

In the past, plaintiffs in the Northern District of California have been able to survive standing challenges when pursuing online service providers for unauthorized disclosure of their personal information. In April 2011, the plaintiff in *Claridge v. RockYou, Inc.* survived a motion to dismiss on standing grounds on the theory that personal information is personal property having monetary value. However, just three days following the successful motion to dismiss in *Low*, Claridge and RockYou settled the dispute (subject to court approval), with RockYou consenting to an injunction requiring two privacy/security audits over the next three years. Moreover, in similar litigation in the Northern District of California, *In re Facebook Privacy Litigation*, the court was less amenable to treating users' personal information stored on Facebook as valuable personal property (for an in-depth discussion of these two cases, see our June 2011 issue of *Socially Aware*).

While courts wrestle with users' attempts to challenge how online service providers use their personal information, both Congress and the World Wide Web Consortium (W3C) are independently moving forward with efforts to create new standards to govern online tracking. In May 2011, Sen. John D. Rockefeller introduced the Do-Not-Track Online Act of 2011, a law that, if enacted, would direct the FTC to adopt rules regarding website compliance with Internet users' activation of a "do not track" preference online. In November 2011, W3C published two "first drafts" for Web standards relating to "tracking preference expression" and how websites may engage with users who have opted into the newly conceived "do not track" user preference. The W3C, which develops Web standards and guidelines for the Web, is building these new privacy standards with the expectation that industry stakeholders such as "browser vendors, content providers, advertisers, search engines" among others will adopt the new standards by mid-2012.

Updated FINRA Guidance on Social Media Websites and the Use of Personal Devices

On August 18, 2011, the Financial Industry Regulatory Authority, Inc. ("FINRA") issued Regulatory Notice 11-39 providing guidance to broker-dealer members on social networking websites and business communications. The notice represents FINRA's first update to its guidance on social media since the release of Regulatory Notice 10-06 in January 2010. Regulatory Notice 11-39 merely clarifies existing guidance; accordingly, it is not likely to result in major changes to current social media policies of member firms.

FINRA also provides some comfort for firms that have a policy of deleting inappropriate third-party content. A firm that has a policy of routinely blocking or deleting certain types of content will not be deemed to have adopted similar content that was neither blocked nor deleted.

Background. To understand the guidance, it is important first to understand the difference between static and interactive electronic communications. In 2003, NASD Rule 2210 (on communications) was amended to include participation in an interactive electronic forum in the definition of "public appearance." Since then, FINRA rules do not require prior approval of postings by member firms or their associated persons on interactive electronic forums. In contrast, static communications or postings are regulated as "advertisements" under FINRA rules and, accordingly, are required to be reviewed by a registered principal. Member firms and their associated persons must distinguish between static and interactive electronic communications.

Recordkeeping. Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110 have long required that a broker-dealer retain electronic communications made by the firm and associated persons that relate to the firm's business (i.e., business communications). The posting of content on a website by a member firm or its associated persons is a communication under the FINRA rules and, accordingly, is subject to applicable FINRA recordkeeping rules. According to FINRA, the determination of whether an electronic communication is related to a firm's business and subject to recordkeeping, is a facts and circumstances assessment. Neither the type of device or technology used to transmit the communication nor the ownership of the device is relevant. Finally, with respect to recordkeeping rules, the requirements are the same for both static and interactive electronic communications.

Analyzing a communication is therefore inherently subjective. FINRA notes that autobiographical information, such as location of employment and job responsibilities, might not be a business communication when included in a resume sent to a potential employer. However, listing products and services provided by a firm would constitute a business communication. Compliance departments must develop policies and procedures to help guide their personnel through the subjective nature of these determinations rather than leaving it to the discretion of individual associated persons or deciding on a case-by-case basis.

FINRA cautions member firms that neither they nor their associated persons may sponsor media sites or use communication devices that automatically erase or delete content. The automatic deletion of content precludes compliance with the recordkeeping requirements. FINRA also cautions that, although third-party posts are generally not attributed to a firm or an associated person, the recordkeeping rules require retention of communications received by a firm or an associated person relating to its business and, thus, third-party posts may be subject to recordkeeping obligations. Firms need to make sure that their associated persons that maintain social media sites do not use the sites for business purposes, and that such associated persons have adequate training and education regarding third-party posts, FINRA rules and firm policies. If the particular social media sites have the relevant compatibility, firms should consider requiring that associated persons include static legends on their media sites warning readers that neither the applicable member firm nor the associated person is responsible for third-party content.

Supervision. NASD Rule 3010 provides that member firms must establish and maintain a system to supervise the activities of each registered representative, registered principal and other associated person, and that the system must be reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. If an associated person wants to use a social media site for business purposes, FINRA rules require that a registered principal should review the site prior to its use, to the extent that the content is static. A site should only be approved for use for business purposes if the registered principal has determined that the associated person can and will comply with all applicable FINRA communication rules, federal securities laws and individual firm policies.

FINRA notes that a registered principal must review an associated person's proposed social media site in the form in which it will be launched and notes that some firms require review by a registered principal of the associated person's initial posting on an interactive forum within the site. Postings on an interactive forum generally do not require prior approval under FINRA rules but, according to FINRA, review of the initial post allows the registered principal to review the site in its final design. Member firms should continue to supervise the site, from time to time, for compliance with applicable rules and federal securities laws after launch.

FINRA explained that interactive content may become static through different acts and that such a change in format would change the treatment of such communications under the rules (for example by taking a "comment" on a Facebook post and copying it as a static Facebook "status update"). FINRA also cautioned firms that, as with any other advertisement under FINRA rules, a registered principal must review material changes to previously approved static posts. Associated persons will need to monitor their sites and registered principals must supervise appropriately to ensure continued compliance.

FINRA also cautions that a firm must follow up on "red flags" that indicate noncompliance by its associated persons. FINRA explained that some firms require that associated persons certify annually, or more frequently, that they are in compliance with supervision rules. It also explained that some firms perform random spot checks of websites to monitor firm policy compliance.

Third-Party Links, Third-Party Posts, and Websites. FINRA explains that a firm may not establish links to third-party sites that the firm knows, or has reason to know, contain false or misleading content, and should not do so when there are red flags to that effect. Further, FINRA advises that under applicable communication rules, a firm may become responsible for content on third-party sites if the firm has adopted or becomes entangled with the content on the third-party sites. A firm may be deemed to be entangled with a third-party site if, for example, the firm participates in the development of content on the third-party site. Also, a firm may be deemed to adopt third-party content if it indicates on its site that it endorses the content on the third-party site. Many social media

sites allow third parties to "recommend" a person and allow users to request recommendations. Member firms should consider prohibiting associated persons from soliciting recommendations. Otherwise, the firm may be deemed to have "adopted" the third-party recommendation.

Firms should consider making sure that links to third-party sites are only accessible through a new window, and that a legend appears on the screen warning the reader that he or she is leaving the firm site and disclaiming any responsibility for third-party content. It is unlikely that such legends will shield a member firm from sanction by FINRA, if applicable, but posting such legends may be effective for limiting liability relating to customer claims. Firms should make sure that their policies relating to social media sites address links to third-party sites.

In addition to adoption and entanglement, if a member firm co-brands a third-party site, it will effectively adopt the content of the entire site. A member firm may co-brand a site by, among other things, placing the firm's logo prominently on the site.

FINRA explains that an associated person may respond to business-related posts by a third-party on the associated person's personal social media site as long as the associated person's firm does not have a policy prohibiting the use of personal social media sites for business purposes. This principle applies to all business-related, but not personal, posts. For example, the associated person may respond to questions regarding securities through his or her site unless prohibited by the applicable member firm. FINRA notes that some firms allow their associated persons to post a non-substantive response to a third-party post and allow pre-approved statements that associated persons may use as a response that direct the third-party to a firm-approved communications medium, such as the firm's e-mail system.

FINRA also provides some comfort for firms that have a policy of deleting inappropriate third-party content. A firm that has a policy of routinely blocking or deleting certain types of content will not be deemed to have adopted similar content that was neither blocked nor deleted.

Google has also agreed to operate an online opt-out service through which individuals can ask for their entire image to be blurred if they still consider themselves to be recognizable on the service, and can request that images of their real property or other assets be blurred as well.

Data Feeds. FINRA cautions that firms must manage data feeds inputted into their websites. As data feeds may contain inaccurate data, firms must be familiar with the proficiency of the vendor providing the data and its ability to provide accurate data. Managing data feeds involves understanding the criteria used by vendors in collecting or calculating the data, regularly reviewing the data for red flags and promptly taking necessary measures to correct any inaccurate data.

Accessing through Personal Devices. FINRA explains that firms may permit their associated persons to use personal devices to access firm business applications and to perform firm business activity. However, FINRA cautions that a firm must be able to retain, retrieve and supervise business communications regardless of the ownership of the device. According to FINRA, it is a good idea for a firm to require that, if possible, separate applications on a device be used for business communications to facilitate retrieval of the business communications without retrieving personal communications. FINRA also notes that an application that provides a secure portal into a firm's communications system is preferable, especially if confidential customer information is shared. If a firm has the ability to separate business and personal communications on a device, and has adequate policies and procedures regarding usage, the firm will not be required to (but may voluntarily) supervise personal communications on the device.

Conclusion. Regulatory Notice 11-39 reaffirms FINRA's general expectations of member firms with respect to business communications. FINRA stressed repeatedly that member firms must have policies and procedures in place that cover the firms' compliance efforts with the communication rules, and that the policies and procedures must include training and education. Of course, the firms' training and education must include training on the firms' policies relating to social media and the need to continuously monitor such sites. Firms should also consider continuous refresher courses for their associated persons to make sure they remain vigilant of the need to consider how continuously changing technologies may be treated under the rules.

Agreement Reached in Belgium on Google Street View Privacy Concerns

2010 and 2011 witnessed Google's rollout of Street View, the search company's mobile panoramic mapping service, in a number of European

countries — but not without challenges to the Internet giant, which has had to enter into a variety of agreements with local European data protection regulators. On the heels of clashes with data protection authorities over alleged unauthorized collection of WiFi data while recording images for Street View, Google's popular service is now subject to a variety of conditions imposed by European authorities.

In January 2011, Belgium's Commission for the Protection of Privacy, the country's data protection authority, published a recommendation (available online in French and in Dutch) on mobile mapping services. That recommendation explained that the Commission considers recorded images of individuals and other related property, such as car license plates and homes, to be personal data — and in some cases, even sensitive personal data, for example, images that show individuals near places of worship or medical centers. The recommendation further stated that Google can legally collect and use this form of personal data on the basis of its legitimate interest in operating Street View; however, use of the data must be proportional, and limited to the provision of Google's Street View service.

Street View launched in Belgium on November 23, 2011. Google has agreed to pixellate/blur all individuals' faces and all car license plates prior to online publication of its Belgian Street View images. (Google reportedly began testing its face-blurring technology for Street View in 2008.) Google has also agreed to operate an online opt-out service through which individuals can ask for their entire image to be blurred if they still consider themselves to be recognizable on the service, and can request that images of their real property or other assets be blurred as well. Google is required to respond to such requests within a reasonable period of time. Google's explanation of "confidentiality" in Street View, as well as Google's instructions on how to request that images be blurred, are available online in French, and the Commission has itself published a comprehensive list of FAQs for individuals about Google Street View and related privacy issues, available online in French and Dutch.

Google has reached a similar agreement (available online in German) with data protection authorities in Germany, where individuals' faces are also blurred and an opt-out service is operated. And in the Czech Republic, where Google was banned in September 2010 from recording Street View images, in May 2011 the data protection authority imposed a detailed list of requirements to which Google must adhere when it resumes its image-gathering, including obligations to lower the height of its Street View cameras, to inform municipal authorities when images of their offices or buildings are being recorded, and to launch an advertising and information campaign in Czech to inform the general public that photographs are being taken.

2011: MOST POPULAR YouTube VIDEOS

1. Rebecca Black's "Friday"
2. "Ultimate Dog Tease" by Talking Animals
3. "Jack Sparrow" by The Lonely Island (feat. Michael Bolton)
4. "Talking Twin Babies" by Randy McEntee
5. "Nyan Cat" by Christopher Torres & Sara Joon
6. "Look At Me Now" by Chris Brown (feat. Lil Wayne, Busta Rhymes)
7. "The Creep" by The Lonely Island (feat. Nicki Minaj & John Waters)
8. Maria Aragon's "Born This Way"
9. Volkswagon Commercial "The Force"
10. "Cat Mom Hugs Baby Kitten" by Anonymous

Source: http://mashable.com/2011/12/20/youtube-2011-most-viewed-videos

Some non-EU countries are moving in a similar direction as well. Israel recently decided to permit Street View, subject to a variety of conditions that include obligations for Google to provide an online opt-out mechanism, to publish information about the service in newspapers and online and to prominently mark its Street View cars. Reportedly, those conditions would also permit Israeli citizens to file civil litigation against Google in Israel.

Northern District of California Court Addresses the Law of the (Virtual) Horse (and Bunny)

Online "virtual worlds," such as Second Life, have their own cultures, customs and economies. This presents new challenges for applying existing intellectual property laws to user-created content in such virtual worlds, as illustrated by a recent case in the Northern District of California, *Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*.

Second Life places users, or "residents," into a virtual world where they participate in a virtual economy, trading virtual goods and services with each other. Residents also have the ability to create new content using a programming language built into Second Life. Under Second Life's Terms of Service, residents retain ownership of the copyright in any content they create. Second Life is thus a breeding ground for digital rights disputes, as residents spend virtual "Linden Dollars"—which can be exchanged for "real world" currency—for virtual goods created by other residents, implicating legally protected rights that have dollar value in the "real" economy. In other words, as one blog describes it, "[w]hile it may be a virtual world, it still has to deal with real-life intellectual property shenanigans."

The dispute in *Amaretto Ranch* concerned the sale of "breedable" virtual animals created and sold to users within Second Life. Ozimals accused Amaretto Ranch of selling "virtual horses" that used the same code used to create Ozimals' "virtual bunnies," thereby infringing Ozimals' copyrights. Ozimals sent a Digital Millennium Copyright Act ("DMCA") takedown notice to Linden Labs, the operator of Second Life, demanding the removal of Amaretto Ranch's virtual horses, sparking a public war of words between Ozimals and Amaretto Ranch.

Amaretto Ranch highlights an important strategic consideration: When a competitor sends out a groundless DMCA notice, should the accused infringer immediately seek judicial intervention or is it better to wait for the service provider to remove the accused materials?

Amaretto Ranch responded by suing Ozimals for violation of Section 512(f) of the DMCA, which provides a cause of action (including recovery of attorneys' fees) for sending a takedown notice containing material misrepresentations. Amaretto Ranch also asserted a state law cause of action for tortious interference with contract based on Ozimals' takedown notice. Amaretto sought and obtained a temporary restraining order and a preliminary injunction requiring Ozimals to withdraw the DMCA notice. Therefore, Linden Labs did not remove any of the allegedly infringing materials from Second Life.

On a first motion to dismiss, the court disposed of Amaretto Ranch's Section 512(f) claim fairly easily, dismissing the claim because Linden Labs had never actually removed the allegedly infringing material. Removal of the allegedly infringing material is a requirement to state a claim under the statute. The court also dismissed without prejudice Amaretto Ranch's claim for tortious interference with contract because it was not "plausibly pleaded."

Amaretto then amended its complaint, and Ozimals filed another motion to dismiss. The amended complaint asserted additional state law claims — defamation, trade libel, intentional interference with contract and interference with prospective business advantage — based on Ozimals' takedown notice. In contrast to the state law claim in the first complaint, which the court dismissed because Amaretto had not pleaded sufficient facts, the amended complaint required the court to consider tougher questions regarding federal preemption of state law claims stemming from a DMCA takedown notice.

Perhaps unsurprisingly, the court followed two previous cases from the Northern District of California holding that Section 512(f) preempts state law claims based on DMCA takedown notices, *Online Policy Group v. Diebold, Inc.* and *Lenz v. Universal Music Corp.* According to the court, *Diebold* and *Lenz* stand for the proposition that a DMCA takedown notification is "a creature of a federal statutory regime, and . . . that regime preempts any state law claim based on an allegedly improper" takedown notice.

Amaretto Ranch tried to distinguish *Diebold* and *Lenz* by pointing out that, in those cases, an actual takedown occurred, while in this case Linden Labs never actually removed the allegedly infringing materials. Therefore, argued Amaretto Ranch, the court should follow *Rock River Comm., Inc. v. Universal Music Group, Inc.*, a case we have reported on previously). In *Rock River*, a Central District of California court

held that the DMCA did not apply to the cease and desist letter at issue and, therefore, the DMCA did not preempt a state law tortious interference claim based on the letter. The *Amaretto Ranch* court, however, did not find this argument persuasive. According to the court, *Rock River* was distinguishable because, in that case, there was no takedown notice under the DMCA in the first place, whereas Amaretto Ranch had plainly alleged that Ozimals takedown notice was "within the ambit of the DMCA."

Based on this analysis, the court held that Amaretto Ranch's state law claims were preempted by the DMCA. Of course, as noted, the court had also dismissed Amaretto Ranch's DMCA claim, leaving Amaretto Ranch without any remedy at all. This outcome reveals how thin the protections against misuse of DMCA takedown notices can be where no removal of the allegedly infringing materials has occurred. As other commentators have noted, the DMCA sometimes does not provide for efficient resolution of copyright disputes. No matter what harm results from the issuance of a DMCA takedown notice, and even if the notice contains flagrant misrepresentations and false accusations of copyright infringement, the *Amaretto Ranch* approach denies the accused party any remedy unless the service provider actually removes the allegedly infringing content. At the very least, *Amaretto Ranch* highlights an important strategic consideration: When a competitor sends out a groundless DMCA notice, should the accused infringer immediately seek judicial intervention or is it better to wait for the service provider to remove the accused materials? If the accused infringer gets an injunction to prevent takedown of the accused material, that success could ultimately preclude any recovery for harm resulting from the notice.

Socially Aware Joins the Social Media Era

As a number of our readers have observed, writing a newsletter about social media is a bit like dancing about architecture. We have been working to change this situation, and are happy to announce the launch of our new *Socially Aware* blog -- please check out the blog at **www.sociallyawareblog.com** and let us know your thoughts! We will still be publishing the newsletter, but we now plan to post articles to the blog as soon as they are in final form, rather than waiting until we have the five or six articles needed to fill out an issue of the newsletter. You can also follow us on Twitter; our Twitter handle is **@MoFoSocMedia**. Thank you for your continued support of *Socially Aware*!

Social Media Law Conference: *Socially Aware* has helped to organize Practising Law Institute's "Social Media 2012: Addressing Corporate Risks" Conference to be held in San Fransisco on February 8, 2012 and in New York City on February 29, 2012. The San Fransisco event will be webcasted. For more information, please click here.

Status Updates

Divorcing spouses Stephen and Courtney Gallion may no longer hold the keys to one another's hearts, but they do have each other's Facebook and dating site passwords after Judge Kenneth Shlug ordered the soon-to-be former couple to exchange their log-on credentials. We have reported on social media discovery issues previously, but this is the first time we have heard of a judge allowing spouses to directly access each other's online dating history. An interesting note: complying with the court's discovery order would seem to violate Facebook's terms of use, which prohibit users from sharing their password information.

It may be true that on the Internet nobody knows you're a dog, but if the U.S. Department of Justice has its way, misrepresenting yourself on the Internet could land you in the pound. The Justice Department is arguing that, in at least some cases, it should be able to prosecute violations of website terms of use — such as using a fake identity on a social networking or dating site — as criminal violations of the Computer Fraud and Abuse Act.

Speaking of false identities, Facebook — which requires users to register with their real names — recently kicked *Satanic Verses* author Salman Rushdie off the social network and then told him that he had to go by his rarely used first name "Ahmed" if he wished to return. Mr. Rushdie complained loudly via Twitter, however, and Facebook soon relented.

Social media without disparaging, inflammatory or defamatory content? Doesn't that sort of defeat the purpose? Not according to the Indian government, which is reportedly asking Internet companies and social media sites to screen user content.

The Stop Online Piracy Act has generated plenty of controversy, but one of the more amusing dust-ups involving SOPA occurred when Rep. Steve King (R-Iowa) tweeted during a hearing that: "We are debating the Stop Online Piracy Act and Shiela Jackson [sic] has so bored me that I'm killing time by surfing the Internet." Rep. Sheila Jackson Lee (D-Texas) did not appreciate being called boring and raised an objection to the Tweet that brought the hearing to a sudden halt.

On the fifth day of Christmas, my true love gave to me... the U.S. FDA's draft guidance on "Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices." The heavily-regulated pharmaceutical and medical device industries have been waiting for detailed FDA social media guidance since at least the FDA's 2009 hearings on social media -- but many are saying that, given the guidance's focus on the narrow (albeit vital) issue of unsolicited requests for information on so-called "off-label" uses, there's still much guidance that needs giving. The draft guidance is open for public comment through 90 days from its December 30, 2011 announcement in the Federal Register.

Heard it from a friend: A U.S. District Court in San Jose, California has denied Facebook's motion to dismiss a lawsuit claiming that the social media giant's "sponsored stories" advertising program, which creates ads based on the "likes" of a Facebook user's friends, violates California's right of publicity statute.

Pleased to meet me: An Israeli man has reportedly changed his name to Mark Zuckerberg after Facebook threatened to sue him over his "Like Store," which sold Facebook "likes" to companies in violation of Facebook's terms of use. So will Facebook sue Mark Zuckerberg?

For your "we saw this one coming" file: An Internet company, PhoneDog LLC, has sued a former employee, Noah Kravitz for $340,000 in connection with an allegedly purloined Twitter account. While employed by PhoneDog, Kravitz sent tweets using the Twitter handle "@PhoneDog_Noah"; after resigning to join a PhoneDog competitor, Kravitz changed the account name to @noahkravitz, and continued to communicate with the over 17,000 people following his tweets. PhoneDog alleges that Kravitz's conduct is analogous to stealing a former employer's customer list. We'll be following this one closely . . .

MoFo Reminders:

- **Did you miss our recent webinar on "Managing the Social Workforce"?** Click here to access the replay of this presentation to hear how to address the challenges (and opportunities) associated with employee social media use.
- **Want a free subscription to *Socially Aware*?** If you are not already on our mailing list, please send an email to us at sociallyaware@mofo.com to be added to the list. To access earlier issues of our newsletter, please visit us at http://www.mofo.com/sociallyaware/.