

# Socially Aware:

# The Social Media Law Update

2011 Best Law Firm  
Newsletter

We welcome you to the latest issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media. In this issue, we discuss recently-issued guidance from the NLRB regarding social media usage in an employment context; a new federal court decision highlighting the need to adopt and reasonably implement a “repeat infringer” policy in order to receive protection under the DMCA safe harbors from copyright infringement claims; and important tips regarding civil discovery of social media activities. We also take a look at two new cases involving CDA Section 230 immunity for Internet service providers who block spam messages from reaching their intended recipients; highlight recent legal challenges to Groupon’s business model; summarize a new legal ethics opinion regarding pretrial searches by litigators of prospective jurors’ social networking sites; and update readers on Google’s ongoing copyright law dispute with the Belgian French-language press. All this plus some surprising statistics on social media usage by B2B companies and Status Updates, our round-up of news items pertaining to social media.

## IN THIS ISSUE

- 2** NLRB Report Provides Guidance to Employers on Social Media Issues
- 2** Rough Waters: Repeat Infringer Policies and the DMCA Safe Harbors
- 4** What Every Company Should Know About E-Discovery and Social Media
- 5** CDA Immunity Gives Social Media Providers Wide Latitude in Combating Spam
- 7** Challenges to Groupon’s Business Model
- 8** You’re Out of Order: Jurors, Social Media and Legal Ethics
- 9** Skirmish in Europe: Google Battles the Belgian Press
- 10** Status Updates

---

## EDITORS

John Delaney  
Gabriel Meister  
Aaron Rubin

## CONTRIBUTORS

Susy Hassan  
J. Alex Lawrence  
Chris Lyon  
Jeremy Merkelson  
Judy Mok  
Sarah Prutzman  
Anthony Ramirez  
Karin Retzer  
Timothy Ryan  
Joan Warrington  
Daniel Westman  
Cecilia Ziniti  
Jesse Soslow (*summer associate*)

---

## NLRB Report Provides Guidance to Employers on Social Media Issues

On August 18, 2011, the National Labor Relations Board's ("NLRB") Office of the General Counsel released a [report](#) discussing the outcome of fourteen cases that its Division of Advice has investigated this year involving social media use in the employment context. While the report does not reflect actual decisions of the NLRB, it does indicate the thinking of the NLRB's Chief Attorney, who sets guidelines for what cases will be presented to the NLRB for litigation and decision. In releasing the report, Acting General Counsel Lafe Solomon [stated](#), "I hope that this report will be of assistance to practitioners and human resource professionals."

In furtherance of Solomon's goal, we have identified the major takeaways of this report, which can be divided into two categories:

**First**, when does employee social media use rise to the level of concerted activity that falls under the protection of the National Labor Relations Act ("NLRA")? The various decisions chronicled in the report provide some guidelines. To begin, social media use is more likely to qualify as protected concerted activity where the employee discusses the terms and conditions of his or her employment in a manner that is meant to induce or further group action. The General Counsel appears more inclined to characterize social media use in this fashion when it either is directed to fellow co-workers, or grows out of an earlier discussion about terms and conditions of employment among co-workers.

On the other hand, employee social media use is unlikely to rise to the level of protected concerted activity where it is best

characterized as an individual complaint about working conditions specific to the employee, and is not directed to co-workers or meant to induce group action.

The report also suggests that employee comments that are "maliciously false," a seemingly high standard, will not be protected under the NLRA and that offensive or inappropriate comments about an employer's clients are also unlikely to be protected.

**Employers should not only avoid such overbroad prohibitions, but should also consider including a disclaimer in their social media policies specifically indicating that none of the prohibitions contained therein should be interpreted to interfere with employee rights under the NLRA.**

**Second**, where will the General Counsel draw the line between a valid and invalid employer social media policy? The report suggests that social media policies will be found to be invalid where they would effectively prohibit employees from engaging in protected activity. For example, the General Counsel found a social media policy to be overbroad where it prohibited "inappropriate discussions" about the company, its management, or its employees because this prohibition encompassed protected concerted activity.

Employers should not only avoid such overbroad prohibitions, but should also consider including a disclaimer in their social media policies specifically indicating that none of the prohibitions contained therein should be interpreted to interfere with employee rights under the NLRA.

At the end of the day, situations must always be examined on a case-by-case basis. However, as the General Counsel investigates more cases and continues to issue guidance, and as the NLRB issues case decisions, the law in this area will quickly develop and produce more tangible guidelines for employers to consider.

## Rough Waters: Repeat Infringer Policies and the DMCA Safe Harbors

Section 512 of the [Digital Millennium Copyright Act](#) ("DMCA") offers various "safe harbors" to online service providers ("OSPs") for claims of copyright infringement against them arising from certain acts of their subscribers and account holders. Section 512 provides that in order for an OSP to qualify for the DMCA's protections, it must satisfy certain requirements. One threshold requirement is that an OSP must have a policy that, under appropriate circumstances, provides for the termination of subscribers and account holders who are "repeat infringers."

Until recently, case law construing the repeat infringer policy requirement Section 512's has interpreted the statute to give OSPs wide latitude in adopting and implementing such policies. However, in a recent opinion, [Flava Works, Inc. v. Gunter](#), a federal district court in Illinois held that an OSP's repeat infringer policy was likely insufficient to afford such the protection of the DMCA's safe harbors because its policy did not consider repeated copyright infringement to be a sufficient basis for termination.

Section 512's statutory requirement for a repeat infringer policy has four parts: (1) the OSP must adopt a termination policy; (2) the adopted policy must provide for termination in appropriate circumstances of subscribers and account holders of the OSP's system or network who are

“repeat infringers”; (3) the OSP must inform its subscribers and account holders about the termination policy; and (4) the OSP must “reasonably implement” the policy.

**Flava Works serves as a reminder to companies operating blogs and websites to confirm that they have adopted and implemented a policy for terminating users engaged in repeated copyright infringement.**

In *Flava Works*, the court issued a preliminary injunction against the defendants, Marques Rondale Gunter (“Gunter”) and his website, myVidster.com. myVidster.com allows users to “bookmark” or “post” video files, thereby embedding the video files from other websites on to myVidster.com. While some of the videos offered on myVidster.com are hosted on its servers, the vast majority are hosted on the servers of third-party websites. Importantly, regardless of where a video is hosted, when it is embedded on myVidster.com, it is not simply linked-to from the site; rather, when users play an embedded video, they remain on myVidster.com while viewing it.

Flava Works, Inc. (“Flava Works”), a producer and distributor of adult entertainment products and the plaintiff in the case, repeatedly asked defendant Gunter to remove its copyrighted content from myVidster.com. The evidence indicated that Gunter would only sometimes comply with these requests to remove Flava Works’ content and, further, did


not terminate any users’ accounts for repeated postings of Flava Works’ content.

In issuing a preliminary injunction against the defendants, the court held that Gunter and myVidster.com were unlikely to succeed in their argument that they were protected by one of the four safe harbor provisions of Section 512. In rejecting their argument, the court did not examine every requirement that a defendant must satisfy in order to receive the protection of Section 512’s safe harbors. Rather, the court focused on Section 512’s repeat infringer policy requirement. Gunter, in explaining the repeat infringer policy of myVidster.com, stated that he believed the term “infringer” only included those users who posted videos from password protected or private websites. He stated, in other words, that an infringer under his policy is not one who posts copyrighted works without authorization, but rather, one who posts videos that are not otherwise available on public websites.

In finding that Gunter and myVidster.com’s repeat infringer policy was insufficient to satisfy the requirements of Section 512, the court noted that “[Gunter’s] understanding of the term ‘infringer’ does not encompass the law of copyright.” Indeed, because myVidster.com’s repeat infringer policy did not actually provide for the termination of repeat copyright infringers, the court held that Gunter and myVidster.com were not eligible for the safe harbor provisions of Section 512.


While *Flava Works* does not offer much guidance as to what an adequate repeat infringer policy might look like, it does offer insight into at least a necessary requirement for such a policy. In particular, the case makes clear that a repeat infringer policy must provide for termination of users for repeatedly violating copyright law; a personal determination of what an individual believes to be proper or improper usage is insufficient to satisfy the requirements of Section 512. If nothing else, *Flava*

## SOCIAL MEDIA STATS ON B2B companies



**86%**


**% of B2B Companies Using Social Media**



**82%**


**% of B2C Companies Using Social Media**

---



**69%**

**% of B2B Companies Shifting Marketing \$ to Social Media**




**67%**


**% Difference in Customer Leads of Blogging B2B Companies vs. Non-Blogging B2B Companies**

---


**26%**




**20%**



**19%**



**The Three Most Popular Social Media Channels for B2B Companies**



**100%**

**% of Fortune 500 companies with executives who use LinkedIn**

**Sources:** <http://www.business2community.com/b2b-perspective/five-awesome-b2b-social-media-statistics-053346> and <http://socialmediab2b.com/2011/05/b2b-social-media-statistics-reports/>



*Works* serves as a reminder to companies operating blogs and websites to confirm that they have adopted and implemented a policy for terminating users engaged in repeated copyright infringement.

Even though *Flava Works* does not explore other qualities that a repeat infringer policy should possess to satisfy DMCA requirements, previous cases have offered guidance on this issue. In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, the court stated that, at minimum, an OSP should terminate users when “given sufficient evidence to create actual knowledge of blatant, repeat infringement from particular users.”

Moreover, the court in *Perfect 10, Inc. v. CCBill, LLC* stated that a policy would be considered reasonably implemented “if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications.” The court went on to note that implementation is reasonable “if, under ‘appropriate circumstances,’ the service provider terminates users who repeatedly or blatantly infringe copyright.”

In an attempt to standardize the repeat infringer policies across Internet service providers (“ISPs”), various large ISPs as well as representatives from the film, music and television industries recently teamed up to create a model repeat infringer policy. The policy, which will be administered by the newly created Center for Copyright Information (a partnership of the groups that produced the model policy), creates a “six strikes and you’re out” rule for copyright violations, with each strike having escalating consequences for the user. While this standardized policy is by no means binding on ISPs, it has received support from the White House.

## What Every Company Should Know About E-Discovery and Social Media

With the exponential growth in the use of social media by individuals and corporations, civil discovery questions inevitably follow. Courts and litigants have been left to grapple with questions regarding the discoverability of data on social media sites and the appropriate scope of such discovery. Although the law will surely evolve in this area, some trends have started to appear. Here are four critical items to keep in mind:

**Content from a party on a social media site may be discoverable even if such party has adjusted privacy settings so that only select individuals can view the content.**

**First**, no one seriously questions that photos, postings, messages, and other information stored on social media sites are open to discovery. Courts have consistently allowed discovery of data on social media sites in cases presenting a range of issues. Although, as discussed in previous issues of this newsletter, seeking to subpoena data directly from Facebook, Twitter, or other social media providers may in many instances run afoul of the Stored Communications Act, courts have allowed discovery directly from parties to litigation where such data is relevant and available.

**Second**, content from a party on a social media site may be discoverable even if such party has adjusted privacy settings so that only select individuals can view the content. Simply because you believe the information is private, does not mean it is protected from discovery.

For example, in a 2010 federal court case in the Southern District of Indiana, *EEOC v. Simply Storage Management, LLC*, the claimants alleged that they suffered from post-traumatic stress disorder as a result of employment discrimination. At the defendant’s request, the court ordered the claimants to produce all relevant “profiles, postings, or messages . . . and . . . applications” as well as photographs and videos on their social media sites. The court found that “a person’s expectation and intent that her communications [on a social media site] be maintained as private is not a legitimate basis for shielding those communications from discovery.” The court considered this simply “the application of basic discovery principles in a novel context.”

Similarly, in a New York case also from 2010, *Romano v. Steelcase Inc.*, the court granted the defendants access to the plaintiff’s “current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information.” The court concluded that allowing the plaintiff to “hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trail.”

**Third**, the fact that a party to litigation maintains profiles on social media sites does not give the opposing party carte blanche to compel broad discovery of the contents of those sites. When it comes to social media sites, courts have been especially wary of providing a license for a fishing expedition. If you are seeking data stored on a social media site, you will probably need to present some basis to suggest that the information is relevant.

For instance, in another recent New York case, *Habib v. 116 Central Park South Condominium*, the defendant condominium in a slip and fall case sought an order compelling the eighty-year-old plaintiff “to provide authorizations for Facebook, MySpace and/or Twitter” accounts that he maintained. The court, however, refused to compel discovery into this tech-savvy octogenarian’s social media usage, finding the defendant did “not offer a reasonable explanation as to why they believe that material information would appear on plaintiff’s social network pages [and that without] the explanation, the requested authorization is a fishing expedition.”

Likewise, in the New York case *McCann v. Harleysville Insurance Company of New York*, the court affirmed an order denying a motion to compel discovery into a litigant’s social media data, finding “defendant essentially sought permission to conduct a ‘fishing expedition’ into plaintiff’s Facebook account based on the mere hope of finding relevant evidence.” Although the universe of reported cases involving discovery from social media sites is rather small, courts have been quick to cut off litigants who simply want to snoop around the opposing party’s social media sites.

In contrast, where a party has been able to establish that the private portion of an opposing party’s social media website is relevant, courts have been willing to permit discovery. For instance, in a Pennsylvania case from earlier in 2011, *Zimmerman v. Weis Markets, Inc.*, the defendant in a personal injury case sought access to the non-public portions of the plaintiff’s Facebook and MySpace pages to refute the plaintiff’s claim that a forklift accident caused serious and permanent impairment to his health and ability to enjoy life. A review of the public portions of the plaintiff’s Facebook page reflected that his interests included “ridin” [sic] and “bike stunts” and included recent photographs of the plaintiff “with a black eye and his motorcycle before and after an accident.” Unsurprisingly, the court permitted the discovery to proceed.

Likewise, in *Romano v. Steelcase Inc.*, the court granted a motion to compel

discovery of the private portions of the plaintiff’s Facebook site where plaintiff’s “public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed.”

**Keep in mind that courts may not look favorably on a request to engage in discovery of social media sites without some indication that they are likely to include relevant information.**

Thus, keep in mind that courts may not look favorably on a request to engage in discovery of social media sites without some indication that they are likely to include relevant information. If you seek to obtain discovery regarding the private portions of the other side’s social media website, you may need to establish that the discovery is warranted. This could be established using public portions of the social media site or perhaps an affidavit from an individual who is a “friend” of the other party and who has had access to the private portions of the website. Establishing such relevance may not be possible in all cases, but you should make every effort to present a detailed showing as to why the discovery is necessary in your case.

**Finally**, if you receive a demand from your adversary for information available on a social media site, merely arguing that all of the data is – or once was – publicly available may not be sufficient. Recent case law suggests that the party maintaining the social media site has the

burden of capturing and producing any relevant content, even when that content is publicly available.

In a recent trade dress infringement case in New Jersey federal district court, *The Katiroll Co., Inc. v. Katiroll and Platters, Inc.*, the plaintiff moved for spoliation sanctions against the defendants after the individual defendant removed his Facebook profile picture, which showed the allegedly infringing trade dress, without preserving the appearance of his Facebook page prior to the change. The defendants argued that a finding of spoliation was unwarranted because the Facebook page was public and the plaintiff could have printed any relevant evidence at any time. The court disagreed, finding “public websites to be within the control of parties who own them” and calling the defendants’ argument “an attempt to ‘pass the buck’ to Plaintiff to print websites that Defendants are obligated to produce.” In this same vein, because of potential hurdles in getting printouts from publicly available social media websites admitted into evidence, you may want to insist on receiving the other party’s social media data directly from that party, even if such data are publicly available.

## CDA Immunity Gives Social Media Providers Wide Latitude in Combating Spam

As we [reported last month](#), the safe harbor in [Section 230](#) of the Communications Decency Act (“CDA”) immunizes social media providers from liability based on content posted by users under most circumstances, but not from liability for content that the providers themselves generate. But what about when providers block Internet traffic such as “spam” – does the CDA immunize service providers from liability for claims related to messages *not* reaching their intended recipients?

In two recent unpublished cases, *Holomaxx Techs. Corp. v. Microsoft Corp.* and *Holomaxx Techs. Corp. v. Yahoo! Inc.*, Judge Fogel of the Federal District Court for the Northern District of California held that the CDA does provide immunity in such circumstances. (Notably, Judge Fogel also decided earlier this year that Facebook postings qualify as “commercial electronic mail messages” regulated under CAN-SPAM, the federal anti-spam statute.) The *Holomaxx* holdings did not break new ground, but the cases clearly show that Section 230 of the CDA provides immunity not just with respect to user-posted content, but also for service providers’ blocking and restriction of messages.

Plaintiff Holomaxx Technologies runs an email marketing and ecommerce business development service. After what it alleged was MSN’s and Yahoo!’s continued refusal to deliver its legitimate emails, Holomaxx sued both companies for state law tort claims alleging interference with contract and business advantage, defamation, false light, and unfair competition, and for federal claims under the Wiretap Act, the Computer Fraud and Abuse Act, and the Stored Communications Act. Seeking both damages and an injunction, Holomaxx claimed that MSN and Yahoo! “knowingly relie[d] on faulty spam filters” and that it was “entitled to send legitimate, permission-based emails to its clients’ customers now.”

In its complaints against Microsoft and Yahoo!, Holomaxx explained that it delivers for its customers ten million email messages a day, including three million to Hotmail/MSN users and six million to Yahoo! users. Holomaxx claimed that it sent only legitimate, requested emails to consenting users and complied with CAN-SPAM. According to Holomaxx, MSN’s and Yahoo!’s email filtering systems began blocking, rerouting, and/or throttling Holomaxx-generated emails to MSN and Yahoo! users, and MSN and Yahoo! ignored its requests to be unblocked and failed to identify specific problems with Holomaxx’s emails. Also according to Holomaxx, MSN and Yahoo! users acted

in bad faith because they did not work with Holomaxx in the manner prescribed by the abuse desk guidelines of the Messaging Anti-Abuse Working Group, to which both companies belong and which Holomaxx characterized as an “industry standard.” Finally, Holomaxx claimed that anticompetitive purposes drove MSN’s and Yahoo!’s blocking, and that the fact that the two companies had initially resumed delivery of Holomaxx emails and then stopped again showed that the companies acted in bad faith.

MSN and Yahoo! moved to dismiss, citing CDA Section 230(c)(2), which on its face immunizes service providers for “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers ... objectionable,” and arguing that the facts that Holomaxx alleged were insufficient to overcome this statutory immunity.

Agreeing, Judge Fogel called CDA immunity “robust” and, citing the Ninth Circuit’s opinion in *Fair Housing Council v. Roommates.com, LLC*, noted that “all doubts must be resolved in favor of immunity.” The court cited Zango v. Kaspersky, where the Ninth Circuit explained that the CDA “plainly immunizes” providers that “make[s] available software that filters or screens material that the user or the provider deems objectionable.” In *Zango*, the Ninth Circuit affirmed the district court’s dismissal of a software maker’s suit against an anti-adware security firm for allegedly making it difficult for users who had installed the security firm’s anti-adware tools to use the plaintiff’s software. However, the Ninth Circuit explained that a provider might lose immunity where it “block[s] content for anticompetitive purposes or merely at its malicious whim.” Under that standard, the question was whether Holomaxx alleged sufficient facts to show that MSN and Yahoo! acted in an “absence of good faith” when they blocked Holomaxx’s emails.

The answer was no. The court discounted Holomaxx’s reliance on the MAAWG guidelines because Holomaxx had not shown them to be an industry standard.

The fact that the companies temporarily resumed delivery of Holomaxx’s emails did not demonstrate an anticompetitive motive because the CDA gives providers wide discretion in deeming content objectionable. As to alleged malice, the court explained that, “[T]o permit Holomaxx to proceed solely on the basis of a conclusory allegation that Yahoo! acted in bad faith essentially would rewrite the CDA.” (Note: On its face, the CDA did not apply to Holomaxx’s Wiretap Act and Stored Communications Act claims; the court dismissed those claims because it found that Holomaxx failed to adequately allege how MSN or Yahoo! had violated those statutes.)

A leading commentator has noted that the Ninth Circuit’s *Zango* case provided website operators a “high degree of freedom to make judgments about how to best serve their customers.” The *Holomaxx* dismissals confirm that point. With social media spam on the rise even as email spam decreases and web-based email in general declines, both the *Holomaxx* and *Zango* cases could assist social media providers in their efforts to prevent unsolicited messages and abuse while at the same time maintaining the instant, social, viral qualities that keep users engaged and advertisers paying.

One final point – as one observer notes, Holomaxx’s compliance with CAN-SPAM, described in great detail in each of the complaints, did not matter to Judge Fogel’s holding. That is, the mere fact that Holomaxx’s marketing messages were legal, did not compel Microsoft or Yahoo! to either deliver those messages or lose CDA immunity. Thus, the court rejected an argument that might have resulted implicitly in the requirements of CAN-SPAM setting a ceiling, rather than a floor, for service providers’ anti-abuse efforts.



## Challenges to Groupon's Business Model

Groupon, Inc. ("Groupon") has become a popular social media phenomenon and formidable online presence offering consumers goods and services at heavily discounted prices since its inception three years ago. Groupon offers daily deals for things to do, see, eat and buy in each of its many local markets – for example, \$100 worth of spa services for \$50 in New York City. Groupon is a collective action platform; if enough people purchase the Groupon coupon for the offered deal, the deal is "on," and customers have a limited window of time in which to purchase the offered product or service and redeem the coupon. Groupon typically splits the proceeds of the deal 50-50 with the merchant. Groupon further raised its public profile by filing for an initial public offering in June 2011.

Of course, as with any successful and lucrative business model, Groupon has quickly attracted a formidable army of competitors (such as LivingSocial, Travelzoo, and, most recently, Google Offers). Groupon, however, has also drawn the attention of state regulators.

Connecticut Attorney General George Jepson has become interested in Groupon and its daily deals because of concerns that expiration dates imposed on some of the Groupon discount offers ("Groupons") sold to Connecticut consumers may violate state law pertaining to gift certificates. In his July 12, 2011 [letter](#) to Groupon, Jepson asked Groupon to provide information about the Groupons, and, in particular, to explain the terms under which Groupons are sold to and redeemed by consumers, how much revenue those sales generate in Connecticut, and how frequently expiration dates are imposed on the sale of goods and services at a discount. Connecticut law provides that gift certificates must not have

expiration dates, and the deal vouchers that Groupon provides to its subscribers may be deemed "gift certificates" under Connecticut law. Many other states have similar laws prohibiting or limiting gift card expirations. The Illinois Attorney General is expected to conduct a similar investigation.

**As with any successful and lucrative business model, Groupon has quickly attracted a formidable army of competitors (such as LivingSocial, Travelzoo, and, most recently, Google Offers). Groupon, however, has also drawn the attention of state regulators.**

In addition, the questions raised by the Connecticut Attorney General regarding the terms under which Groupons are sold to and redeemed by consumers indicate that the Attorney General could be formulating an Unfair and Deceptive Acts and Practices ("UDAP") case against Groupon. For example, the Connecticut Attorney General has asked Groupon to identify "the portion of such revenue attributable to such goods and/or services for which 'Groupons' discounts expired prior to consumer use (i.e., revenue derived from purchasers who obtained but were unable to use such 'Groupons' for discounts on the purchase of goods or services because expiration dates had passed)." Groupon also received a request for information from Reps. Ed Markey (D-Mass.) and Joe Barton (R-Tex.) on July 21, 2011, regarding Groupon's privacy policy and data security practices, shortly after Groupon announced its plans to collect

more information regarding its users and to share such information with its business partners.

Groupon also has been named as a defendant in a number of class action lawsuits from customers across the United States alleging that Groupon violates consumer protection laws by setting expiration dates and other limits on its daily deals. Consumers have accused Groupon of violating the Credit Card Accountability Responsibility and Disclosure Act ("CARD Act") and the Electronic Funds Transfer Act ("EFTA"), 15 U.S.C. § 1693 *et seq.*, which specifically prohibit the sale and issuance of gift certificates with expiration periods of less than five years. However, Regulation E, 12 C.F.R § 205, issued pursuant to the EFTA, also provides that a "loyalty, award, or promotional gift card" would not be categorized as a gift card or gift certificate for purposes of Regulation E. An argument could be made that Groupon deal vouchers fall under this Regulation E exclusion. In the event that the Groupon deal vouchers would qualify as "gift certificates" pursuant to the federal gift card laws and implementing regulations, Groupon would have to consider the minimum five-year expiration date requirement, which could alter its business model, since Groupon deal vouchers typically expire between six and eighteen months after purchase. Classifying the Groupon deal vouchers as gift certificates could open a Pandora's box of both federal and state laws to which Groupon would be subject based on its business model.

Groupon has attempted to address these possible legal issues relating to expiration dates by separating the "purchase value" from the "promotional value" in its Groupons. According to Groupon's Terms of Sale found in Section 7 of Groupons [Terms of Service](#), each Groupon deal voucher consists of a purchase value (the discounted amount that the customer actually pays in exchange for the goods and services) and a promotional value (the difference in value between the full

offer value and the purchase value). The purchase value does not expire until it is used or refunded. Conversely, the promotional value expires on the date stated on the Groupon deal voucher unless applicable law prohibits the promotional value from expiring. Only time will tell whether Groupon's attempts at complying with these possible gift certificate law issues will be sufficient to satisfy state regulators' concerns regarding consumer protection or result in the dismissal of the currently pending class actions.

## You're Out of Order: Jurors, Social Media and Legal Ethics

The Internet and, in particular, social media have changed the landscape of federal and state jury instructions, which now prohibit jurors from conducting independent research on the Internet, from sending emails, texts, Facebook postings, tweets or other electronic communications conveying developments in a trial or in deliberations, and from using mobile cameras to record courtroom proceedings. Recently, the [New York County Lawyers Association \(NYCLA\) Committee on Professional Ethics](#) ("Committee") weighed in on a new area involving jurors and social media: lawyers' investigation of jurors' Internet and social media postings before, during and after a trial.

Through [Formal Opinion No. 743](#), issued on May 18, 2011, the Committee opined that it is proper and ethical under the [New York Rules of Professional Conduct \(RPC\)](#) 3.5, 4.1, and 8.4 for a lawyer to undertake a pretrial search of a prospective juror's social networking sites, provided that there is no contact or communication with the prospective juror and the lawyer does not seek to "friend" jurors, subscribe to their Twitter feeds, send tweets to the jurors or otherwise contact them. The Committee also opined that, during the evidentiary or

deliberation phases of a trial, a lawyer may visit a juror's publicly available Facebook, Twitter and other social networking sites, but must not "friend," send tweets or email messages to, or otherwise communicate in any way with a juror, or "act in any way by which the juror becomes aware of the monitoring." Moreover, the lawyer may not make any misrepresentations or engage in deceit, indirectly or directly, in reviewing jurors' social networking sites. The Committee noted that, in the event a lawyer learns of juror misconduct, the lawyer may not unilaterally act upon that knowledge (e.g., in settlement discussions with the opposing side), but must promptly comply with Rule 3.5(d) and inform the court of such misconduct.

**A lawyer may visit a juror's publicly available Facebook, Twitter and other social networking sites, but must not "friend," send tweets or email messages to, or otherwise communicate in any way with a juror, or "act in any way by which the juror becomes aware of the monitoring."**

As the Committee's opinion makes clear, there is a tension between avoiding *ex parte* contact with jurors and keeping the court reasonably informed about juror misconduct. On one hand, attorneys must avoid all contact with jurors through their social media sites; on the other hand, attorneys must inform the court immediately if they learn through social media of jurors' misconduct. There is little doubt that much juror misconduct goes unreported because attorneys are forbidden from accessing jurors' revelatory non-public musings undertaken through social media.

The Committee's fundamental assumption is that active monitoring of which a juror becomes aware constitutes an impermissible communication, as it may tend to influence the juror's conduct with respect to the trial at hand. But it will be interesting to see how the proscription that attorneys must not "act in any way by which the juror becomes aware of the monitoring" plays out in real life, given the complexity and continuing evolution of social media services – services that regularly update their respective interfaces, features, privacy controls and notification options.

Take, for example, Twitter, which currently lets each account holder set his or her notification settings to notify the account holder every time he or she is "followed" by someone new. However, in order to read a Twitter user's tweets, one only needs to visit the user's Twitter feed URL, not affirmatively "follow" the user – with the important exception of Twitter users who have used the site's account settings to enable "Tweet privacy" and ensure that only pre-approved individuals can see their Tweets.

And consider LinkedIn, which currently offers a "[Who's Viewed Your Profile?](#)" feature. LinkedIn's account settings enable each account holder to select which pieces of his or her profile information will be visible to another LinkedIn user whose profile he or she visits; settings include "Your name and headline (Recommended)," which would display the visiting account holder's name, title, company and general location, "Anonymous profile characteristics such as industry and title," and "You will be totally anonymous."

These and other social media services may well change over time. Thoughtfully, the Committee's opinion notes that it "is intended to apply to whatever technologies now exist or may be developed that enable the account holder to learn the identity of a visitor."



## Skirmish in Europe: Google Battles the Belgian Press

In the [June 2011 issue](#) of *Socially Aware*, we reported on a Brussels Court of Appeal ruling in favor of Copiepresse, the Belgian association for the protection of French-language press copyright, in a case against Google. To recap, on May 5, 2011, the Brussels Court of Appeal upheld an earlier ruling that Google had infringed copyright when it displayed links to and extracts of online newspaper articles that were usually only available to paying subscribers of the online newspapers at issue.

In reaction to the May 5th ruling, Google removed all Belgian French-language daily newspapers from its search index and cache on July 15, 2011. As a result, the websites for Belgian newspapers *Le Soir*, *La Libre Belgique*, *Sudpresse* and *l'Echo* were unavailable in Google's search results on both Google News and Google's main search page. Belgian national *Le Soir* took issue with Google's actions and, in an article dated July 16,

2011, [complained](#) that Google made "Belgium newspapers disappear." Within hours of learning about Google's actions, Copiepresse entered into negotiations with Google, and reached an agreement resulting in the news sites and certain related content being restored to Google search results by July 18, 2011. The agreement [reportedly](#) allows Google to link to the online news sites in Google's search results, but not to reproduce extracts of articles in Google's news service.

Google's actions were based on its literal interpretation of the Court of Appeal's ruling, and in the company's defense, a Google spokesperson stated that Google was merely eliminating all risks of incurring fines of EUR 25,000 (approximately USD 35,600) per day for non-compliance with the ruling. Google [sought](#) the waiver of potential penalties with respect to restoring links to the news sites on its search service. Nevertheless, Google's conduct has been [characterized](#) by observers as an effort to "punish" Belgium's French-language press for objecting to Google's business practices, and sent a stark warning to online news publishers, many of whom depend on Google-generated traffic for customers and ad revenues.

All this comes at a time of heightened antitrust scrutiny for Google in the EU. For example, [German](#) and [Italian](#) press associations have already brought antitrust-related complaints against Google. Also, portions of the German complaint were [referred to](#) by the European Commission competition service, which opened formal proceedings against the search giant for alleged abuse of dominant position in November 2010. The EU investigation focuses on Google's alleged lack of transparency in rankings, biased search results and unfair terms and conditions. Such cases typically take years to conclude.

In any event, this matter is far from over. Google has not yet filed an appeal against the Brussels Court of Appeal's ruling, and has until December 2011 to do so.

---

**If you wish to obtain a free subscription to *Socially Aware*, please send an email to [sociallyaware@mofocom](mailto:sociallyaware@mofocom). To review earlier issues of *Socially Aware*, visit us at <http://www.mofocom/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 eight 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.

# Status Updates

Your tax dollars at work: The IRS has issued a [new personal computer use policy](#) that prohibits employees from using government computers to access social networking sites. Other personal-use websites, such as Craigslist, dating sites, and pornographic sites are also off-limits according to the new policy.

Not wanting to be outdone by the IRS, the Department of Veterans Affairs has also issued a [new policy](#) providing guidelines to ensure the privacy and security of personal information that appears in social media used by the department. The policy includes directives regarding privacy policies, protection of First Amendment rights, regulatory compliance, and removal of inappropriate user comments. Interestingly, the VA's [announcement](#) of the new policy states that the VA has "over 100 Facebook pages, more than 50 Twitter feeds, two blogs, a YouTube channel, and a Flickr page."

LinkedIn, which has largely avoided the privacy-related controversies that have plagued other social networking sites, [announced](#) that it would not move forward with a plan to place users' photos and recommendations in advertising displayed on its network. LinkedIn's head of marketing solutions products told users "we hear you loud and clear" after the company received complaints about the plan.

Initial reports indicated that the FTC was preparing to harsh Ashton Kutcher's buzz. [The word on the street](#) was that the actor was facing questions from the Man about his failure to disclose his investments in Internet companies profiled in the online-only issue of Details magazine that he edited and posted on social networking sites. Luckily for Mr. Kutcher, the bad vibes were dispelled when an FTC spokesman subsequently [announced](#) that everything was copasetic and there would be no investigation.

Feeding our insatiable appetite for social networking statistics, a [new study](#) suggests that user engagement with certain Facebook activities may be declining. According to the study, Facebook activities such as virtual gifting, messaging to friends, joining a group, searching for new contacts, installing an app, and instant messaging are all on the decline.

On the other hand, [comScore's July 2011 traffic numbers](#) show that Facebook and

Twitter both drew record traffic in terms of unique U.S. visitors for the month. Facebook saw 162 million unique visitors, while Twitter drew 32.8 million uniques in July.

On the third hand, a recent [Pew Internet survey](#) indicates that social media use is not (yet) ubiquitous in the U.S., with only half of U.S. adults reporting that they use social media. In the U.K., results of the [annual survey](#) from the Office of National Statistics indicate that 57% of the U.K. population aged 16 and over is now using social media. All of these statistics can get confusing, but one thing is certain: social media either is or is not taking over the world.

Facebook announced [significant changes](#) regarding privacy, content sharing, and tagging. Among other things, individual items of content on a user's profile page now have drop-down menus that let the user change who can see the content – the public, just friends, or custom settings. Previously, users had to go to the separate privacy settings page to make such changes.

In our last issue of *Socially Aware*, we reported that William Shatner's Google+ account was temporarily suspended for an unspecified rule violation. Sex and technology blogger Violet Blue ran into [similar problems](#) recently when her Google+ account was shut down because Google mistakenly believed that she had not used her real name to sign up for the service. Google apologized for the error, but for the time being is sticking to its [requirement](#) that users identify themselves with their real names when using the social network.

Bringing to mind War's 1975 hit "[Why Can't We Be Friends](#)," a Missouri teachers union is [suing](#) to block the "Amy Hestir Student Protection Act," which would restrict contact between teachers and students on social media sites. According to the teachers, the new law violates teachers' constitutional rights to free speech and association.

[Reports](#) are that Facebook and Lamebook have settled their trademark dispute with an agreement that lets the parody site continue to operate under its current name, as long as it adds a disclaimer to its website and does not seek to register its name as a trademark. Our previous coverage of the Facebook/Lamebook dispute can be bound in the [December 2010 issue](#) of *Socially Aware*.

Expanding upon the Ninth Circuit's ruling in *United States v. Nosal*, Judge Jeremy Fogel of the Northern District of California recently [held](#) that an Internet marketer may be liable under CAN-SPAM and the Computer Fraud and Abuse Act, and for fraud, based on using Facebook to conduct advertising campaigns in violation of Facebook's terms of service. Judge Fogel's most recent ruling in *Facebook Inc. v. MaxBounty Inc.* follows his prior order in the case, which we covered in the [April 2011 issue](#) of *Socially Aware*.

Freedom Watch founder Larry Klayman apparently felt that the New York federal judge who tossed his [\\$1 billion suit](#) against Facebook, arising from allegations that Facebook was too slow to remove an anti-Jewish page from its site, showed a bit too much *chutzpa*. According to reports, Klayman stated, "In my 35 years of legal practice, I've seen judges dismiss cases like this, thinking they can do whatever they want. But they have to obey the law like we do." A Facebook representative, on the other hand, asserted that "lawsuits such as this – which seek to hold Facebook liable for failing to screen and remove content posted by its users – are precisely what the CDA was enacted to foreclose."

Loose tweets sink claims: Orlando Magic point guard Gilbert Arenas [sued](#) in California federal court to prevent broadcast of the VH1 reality TV show "[Basketball Wives: Los Angeles](#)". The athlete claimed that the show improperly used his name and likeness to imply that he was involved in the program. District Judge Dolly M. Gee [held](#), however, that Arenas' prolific tweets, in which he described various details of his daily activities to thousands of followers, meant that he could not persuasively argue that his personal life is not a matter of public concern. Publication of matters in the public interest is a First Amendment-based defense to California's right of publicity law. Free speech advocates and reality TV fans everywhere are no doubt breathing a sigh of relief.

The Distilled Spirits Council of the United States has issued new self-regulatory industry [guidelines](#) for advertising of alcoholic products on social media websites. According to the new guidelines, only social media websites where at least 71.6% of the audience is reasonably expected to be age 21 or older will be permitted to advertise such products.