

# Socially Aware: The Social Media Law Update

2011 Best Law Firm  
Newsletter



## IN THIS ISSUE

- 2** Can “Friending” Employees Lead to Legal Headaches?
- 2** Open Kimono: Court-Compelled Discovery of Non-Public Social Media Pages
- 4** Employee Non-Compete and Non-Solicitation Agreements in the Social Networking Era
- 5** A Copyright Troll’s Last Stand?
- 7** Facebook Not “Liked” in Europe, Overhauls Its Privacy Settings
- 9** Ninth Circuit Follows *eBay v. MercExchange* and Second Circuit on Preliminary Injunctions for Alleged Copyright Infringement
- 10** The FTC Proposes Changes to Its COPPA Rule – And Why Every Website Operator Should Pay Attention
- 12** Status Updates

In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we discuss employment law considerations in “friending” a colleague; how an ex-employee’s social media use can run afoul of non-compete or non-solicitation obligations to a former employer; a recent court decision in which a plaintiff was ordered to disclose her Facebook and MySpace passwords to opposing counsel; Facebook’s privacy-related headaches in Europe; an overview of copyright troll Righthaven’s recent string of defeats; an important decision in the *Perfect 10 v. Google* litigation regarding the availability of injunctive relief in copyright infringement actions; and FTC efforts to significantly expand the scope of what constitutes “personal information.” All this, plus statistical snapshots of social media trends and *Status Updates*, our round-up of social media news items.

## EDITORS

John Delaney  
Gabriel Meister  
Aaron Rubin

## CONTRIBUTORS

Seth Graham  
Susy Hassan  
Emily Hutters  
Jacob Kaufman  
Julie O’Neill  
Karin Retzer  
Eric Akira Tate  
Marissa Coleman (*summer associate*)

## Can “Friending” Employees Lead to Legal Headaches?

Online social networking, and its capacity to connect our professional lives to our personal lives, have introduced a variety of new legal issues in the workplace – issues that we explore regularly in *Socially Aware*. Many managers and supervisors have connected with subordinates on social networking sites, and have likely wondered about the practical and legal implications of doing so. Applying long-standing legal concepts to this new context, a number of potential issues stand out.

First, when a supervisor connects with a subordinate on a social networking site such as Facebook or Twitter, that supervisor may be put on notice of legally protected information. For example, an employer may learn of an employee’s political affiliation, religious beliefs, sexual orientation, or health information. If an adverse employment decision is made against an employee after the employer discovers such information, it may appear as though the action was motivated by unlawful discrimination. Managers may also see employees’ job-related postings, and find themselves in the difficult position of trying to determine how to address poor judgment without running afoul of legal protections for employee

**Many managers and supervisors have connected with subordinates on social networking sites, and have likely wondered about the practical and legal implications of doing so.**

speech. (See our [October 2011 issue of \*Socially Aware\*](#) for more information regarding such protections.)

Second, employers could become more vulnerable to discrimination and harassment claims based on a supervisor’s social media-related interactions with subordinates. For example, a supervisor might be discriminatorily selective with respect to those subordinates whom he “friends” via Facebook. Although a discriminatory “friending” pattern may be insufficient standing alone to establish legal liability, it might be used as a piece of corroborative evidence against the employer.

Further, people often say things in a personal capacity that would not necessarily be appropriate in the workplace; if a supervisor exhibits a sexist or racist point of view on his Facebook page, for example, this could add fodder to a claim of discrimination or harassment. On the flip side, supervisors may have an affirmative duty to take action if they learn of harassing social media-related postings that affect employees.

Finally, managers should consider that subordinates may feel pressured to accept a “friend” invitation, and that, if such invitation is accepted, the manager may end up learning more than he or she wanted to know about the accepting employee’s weekend plans, job-related gripes, status updates and so forth. In some cases, a manager may find that less is more, when deciding whom to “friend” at work.

We here at *Socially Aware* do not want to be known as killjoys; we are big users of social media, and are loath to discourage “friending” of one’s colleagues or anyone else. But with the explosive growth of social media blurring the traditional boundaries between one’s professional life and one’s personal life, employers should at least be aware of potential risks issues in “friending” employees. One does not need to be [Nostradamus](#) to predict a coming wave of employment-

**One does not need to be Nostradamus to predict a coming wave of employment-related claims focusing on social media-related interactions between supervisors and subordinates.**

related claims focusing on social media-related interactions between supervisors and subordinates.

## Open Kimono: Court-Compelled Discovery of Non-Public Social Media Pages

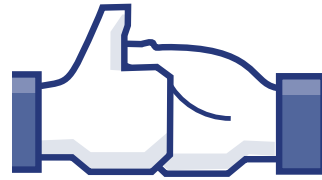
Due to the widespread popularity of social networking sites (“SNS”), courts have had to determine how the rules of discovery apply to content stored on such sites. In addressing this issue, many courts have required parties to provide opposing counsel the SNS content – such as emails and Facebook wall postings – that is relevant to the action, but have generally left SNS account owners in control of access to their accounts. For example, a [Nevada district court](#) denied a defendant’s motion to compel the plaintiff to grant the defendant access to the plaintiff’s MySpace account in order to obtain allegedly relevant communications. Instead, the court determined that the “proper method for obtaining such information” was to serve a “properly limited” request for the production of relevant content. In a case where a plaintiff put the content of her former Facebook account and her state of mind

at issue, a [Connecticut district court](#) required her to produce to the defendant all of the printouts of her account, which had been provided to her by Facebook, after an *in camera* review demonstrated that her initial determination of the relevancy of this information was too narrow. Although this decision may seem far-reaching, the defendant still had to rely on the plaintiff for production of the requested discovery.















Courts in New York and Pennsylvania, however, have expanded the methods of disclosure available to defendants for the discovery of SNS content. In [Romano v. Steelcase](#), as discussed in a [previous issue of Socially Aware](#), a New York trial court ordered the plaintiff to execute the necessary consent and authorization for the operators of Facebook and MySpace to provide the defendant with access to the plaintiff’s personal accounts. And a recent Pennsylvania decision, while relying on [Romano](#), appears to have gone even further than the New York court.

In [Zimmerman v. Weis Markets](#), the Pennsylvania trial court required disclosure to opposing counsel of the plaintiff’s passwords, user names and log in names in order to provide access to the non-public portions of the plaintiff’s personal Facebook and MySpace profile pages. Zimmerman, a former employee of Weis Markets, had brought an action seeking damages for injuries resulting from an on-the-job accident. He claimed both embarrassment from the subsequent scarring and that “he ha[d] sustained a permanent diminution in the ability to enjoy life and life’s pleasures.” Upon review of the public portion of Zimmerman’s personal Facebook and MySpace pages, Weis Markets discovered what it believed to be evidence that contradicted the claims – photographs taken after the accident depicting Zimmerman with his motorcycle and wearing shorts that left the scar on his leg “clearly visible.” The *Zimmerman* court determined that,

### Big Spenders: Social Media Brand Fans Spend More Than Non-Fans



#### PRODUCT SPENDING IN MILLIONS

	Facebook Fan	vs.	Non-Fan
<b>McDonald’s</b>	\$310.18	 	\$150.39
<b>Starbucks</b>	\$235.22	 	\$110.95
<b>Victoria’s Secret</b>	\$229.04	 	\$152.97
<b>Nike</b>	\$205.02	 	\$83.69
<b>PlayStation</b>	\$188.02	 	\$121.61
<b>Motorola</b>	\$160.01	 	\$69.09
<b>Red Bull</b>	\$113.38	 	\$60.83

Sources: <http://www.mofo.com/files/Uploads/Images/111018-MoFo-Tech-Fall-Winter-2011.pdf> (Page 17)

“[b]ased on a review of the publicly accessible portions of [Zimmerman’s] Facebook and MySpace accounts, there was a reasonable likelihood of additional relevant and material information on the non-public portions of these sites.”

In response to Zimmerman’s argument that “his privacy interests outweigh[ed] the need to obtain the discovery material,” the court determined that since he had voluntarily posted all of the pictures and information on his Facebook and MySpace pages and intended to share them with other users of the sites, “he [could not] now claim he possesse[d] any reasonable expectation of privacy to prevent Weis Markets from access to such information.” Further, the court held that “[w]ith the initiation of litigation to seek a monetary award

based upon limitations or harm to one’s person, any relevant, non-privileged information about one’s life that is

**The court required disclosure to opposing counsel of the plaintiff’s passwords, user names and log in names in order to provide access to the non-public portions of the plaintiff’s personal Facebook and MySpace profile pages.**

shared with others and can be gleaned by defendants from the internet is fair game in today's society."

Commentators disagree on what *Zimmerman* ultimately means. One [commentator](#) suggests that such access is "equivalent to turning over a personal diary." [Another](#) explains that "forcing a party to hand over his or her log-in information is *not* the correct result," as it has the potential to provide the other side with access to irrelevant, non-discoverable, and/or private information. On the other hand, one [commentator](#) maintains that the policy "makes sense," arguing that "if there is proof of relevant information contained within a social media account, then that account should be accessible by the side seeking it." [Another](#) observes that, although these pages should be discoverable to an extent, the problem will be in deciding "where to draw the line," and expressed concern that parties would abuse such a rule as a way to wear down the opposing side. With such a mix of reactions, the issue is likely to become a hot topic as other courts determine whether to follow suit.

## Employee Non-Compete and Non-Solicitation Agreements in the Social Networking Era

Employers have long used non-compete and non-solicitation agreements to prevent former employees from taking unfair advantage of confidential information, including client information, to which they received access during their employment. The growth of social media, however, is raising complex new issues for employers seeking to protect such company confidences from misuse by ex-employees. For example, if a former employee subject to a non-compete or non-solicitation agreement connects with

a company client or former coworker on LinkedIn, could such connection result in a breach of the agreement?

Although there has been little definitive guidance from the courts to date, these issues have started to appear more frequently in litigation. In March 2010, for example, TEKsystems filed a [lawsuit](#) against a former employee for violating a non-compete and non-solicitation agreement based on her use of LinkedIn. TEKsystems [alleged](#) that the former employee violated the agreement when she "connected" with one of the company's contract employees on LinkedIn, asked whether he was "still looking for opportunities," and invited him to "come visit [her] new office and hear about some of the stuff [they] are working on." No ruling was issued, as the parties resolved the matter prior to adjudication; the case, however, is a reminder of just how easy it is for departing employees to connect with former colleagues and clients via LinkedIn and similar social media platforms, possibly in violation of their contractual obligations to former employers.

Employers seeking to enforce restrictive covenants may be interested to learn that at least one court has ruled that an ex-employee's use of social media did violate a non-solicitation agreement. In *Amway Global v. Woodward*, a former employee argued that his blogs and website postings could not establish violations of the nonsolicitation agreement because "such passive, untargeted communications fail as a matter of law to qualify as actionable solicitations." The Michigan district court rejected this reasoning, noting that "common sense dictates that it is the *substance* of the message conveyed, and not the medium through which it is transmitted, that determines whether a communication qualifies as a solicitation."

The *Amway* court further confirmed that "communications qualifying as solicitations do not lose this character simply by virtue of being posted on the Internet." Indeed, the *Amway* court found that the ex-employee's posts could constitute a solicitation even where the hosting site's

**If a former employee subject to a non-compete or non-solicitation agreement connects with a company client or former coworker on LinkedIn, could such connection result in a breach of the agreement?**

readership is "diffuse and uncertain." Specifically, in *Amway*, the posting was viewed by nearly 100,000 people and the court still found that it qualified as a solicitation.

Still, whether a particular use of social media can rise to the level of a "solicitation" is fact dependent. Just as a telephone call, email, or meeting can be appropriate or inappropriate depending on its substance, some social media communications will be in breach of non-solicitation agreements while others will not. For example, in *Amway*, the court held that the former employee violated his non-solicitation agreement when he posted on his blog that he had decided to join a competitor and stated, "If you knew what I knew, you would do what I do." Although this posting was not directed at any particular individual, the court held that in light of its content, it "would readily be characterized as [a] solicitation" as it could clearly be read as an "invitation for the reader to follow his lead and join" Amway's competitor. On the other hand, had the former employee simply posted a neutral announcement indicating his decision to join a competitor, it is unclear whether the *Amway* court would have deemed the ex-employee to be in breach of his non-solicitation agreement.

We note that the *Amway* court tailored its analysis to the language of the governing

agreement and found that, because the agreement prohibited employees against “encourag[ing], solicit[ing], or otherwise attempt[ing] to recruit or persuade” others to compete, it was “immaterial” whether any such attempt to do so was successful. Thus, one way for employers to address the current ambiguity as to what kinds of social media use will violate a non-solicitation agreement may be to include a provision expressly prohibiting the use of social media for improper solicitation and outlining the prohibited conduct. If the agreement specifically prohibits the former employee from initiating contact with former coworkers or clients through social media sites such as LinkedIn, a court, as in *Amway*, may be more inclined to find that a simple request to connect breaches the agreement.

Further, as part of a broader trade secrets protection program, employers can use confidentiality agreements as a step toward avoiding the loss of trade secret status. In order to address the particular risk of proliferation of confidential information through social media, employers can maintain strong confidentiality agreements that incorporate provisions explicitly regulating employee social media use as it pertains to confidential information. Such agreements should make clear that such information is the employer’s property and is to be protected as such, especially online. Although there may be concerns about regulating employee social media use (e.g., free speech, concerted activity, and privacy law considerations that are outside the scope of this article), it is clear that employees have no greater right to breach a confidentiality agreement through social media than they otherwise would if not using social media. The bottom line is that the fact that an improper disclosure may occur through a blog or other social media service does not somehow exempt that disclosure from the reach of a lawful confidentiality obligation.

While social media presents new challenges to employers who seek to maintain the confidentiality of sensitive

information and prevent unfair competition by departing employees, the legal issues arising in the context of social media in many respects are not so different from those we have seen in the past. These cases will likely continue to turn on the particular facts presented. With that said, certain themes appear to be developing:

- First, while protecting confidential information as trade secrets may be more challenging with the proliferation of social media sites, employers can support their efforts to do so by using confidentiality, non-compete (where legally permitted), and non-solicitation agreements.
- Second, having clear policies may help employers regulate social media use, particularly where such policies make clear that disseminating confidential information by posting online, including on their own accounts on sites such as Facebook and LinkedIn, is strictly prohibited.
- Finally, an employee cannot do through social media what he or she could not do otherwise.

To quote from the *Amway* decision, “it is the substance of the message conveyed, and not the medium through which it is transmitted,” that carries weight.

## A Copyright Troll’s Last Stand?

Suits by so-called “[copyright trolls](#)” are of keen interest to operators of social media sites, given that user-generated content, or, as some call it, “user-uploaded content,” is a cornerstone of the social media experience. In the [April 2011 issue](#) of *Socially Aware*, we reported on a recent string of lawsuits filed by Righthaven, a company in the business of acquiring third-party copyrights for the purposes of identifying and bringing suit against possible infringers. In that article, we described several recent Righthaven claims against bloggers, forum posters, and other social media users based on

their reposting and (re)use of online content. We also foreshadowed the possible demise of Righthaven’s legal strategy, noting that courts appeared to be concerned that Righthaven’s only interest in the copyrights at issue might be a financial one – a concern supported by an “assignment” of these copyrights to Righthaven that the [Electronic Frontier Foundation](#) (“EFF”) called “[a sham](#).”

Recently, other courts presiding over Righthaven lawsuits have addressed the EFF’s allegations, specifically, regarding the nature and manner of the assignment to Righthaven of the allegedly infringed copyrights, and the implications of that assignment for Righthaven’s standing to sue.

Standing to sue for copyright infringement is described in the U.S. Copyright Act (the “Act”). Under [Section 501\(b\)](#) of the Act, only the legal or beneficial owner of an exclusive right in a copyright is entitled to sue for infringement. This requirement was included in the Act both to protect alleged infringers against a multiplicity of lawsuits and to ensure that copyright owners are made aware of, and given the opportunity to participate in, lawsuits affecting their legal interests. Although exclusive rights afforded to copyright owners under [Section 106](#) of the Act are “divisible” and may each be assigned or transferred to third parties individually or collectively, the right to sue is not one of those enumerated exclusive rights. Therefore, an entity like Righthaven may only obtain the right to sue for infringement if a copyright owner also assigns one of its Section 106 exclusive rights in the copyright at issue (further, that entity may only obtain the right to sue for past infringement if the assignee expressly assigned such right).

Righthaven’s standing to sue under Section 501(b) was precisely the target of the EFF’s and Democratic Underground’s allegations in *Righthaven v. Democratic Underground*, one of the actions referenced above. Righthaven had brought suit alleging that a message-board user, by posting four paragraphs

from a 34-paragraph story from the *Las Vegas Review-Journal* (“LVRJ”) on the Democratic Underground site, had infringed “Righthaven’s” copyright. Righthaven alleged that it had acquired, via an assignment from Stephens Media LLC (“Stephens Media”), publisher of the LVRJ and Righthaven’s original business partner, the rights in the underlying copyrights that were necessary for Righthaven to bring suit. (Righthaven has made the same or similar claims in most of the over 270 lawsuits that it has filed to date.)

In *Democratic Underground*, the court noted that the assignment purported to transfer to Righthaven all copyrights necessary for Righthaven to be recognized as the owner of the subject works for the purpose of being able to seek redress for infringement; however, the assignment did not assign to Righthaven a specific exclusive right. Further, in discovery, Righthaven disclosed to Democratic Underground a “Strategic Alliance Agreement” (“SAA”) that had been entered into between Righthaven and Stephens Media before the assignment at issue and which, by its terms, governed all subsequent assignments between those parties. Section 7.2 of the SAA stated that notwithstanding any assignment, Stephens Media retained the exclusive license to exploit each purportedly “assigned” copyright for any lawful purpose, and that “[Righthaven] shall have no right or license to Exploit or participate in the receipt of royalties from the Exploitation of the [assigned copyrights] other than the right

to proceeds in association with a [recovery in an action for infringement].” The SAA also gave Stephens Media the right to terminate any such assignments in good faith on notice to Righthaven, and entitled Stephens Media to a 50% share of any awards received by Righthaven in lawsuits that Righthaven later filed based on the subject copyrights.

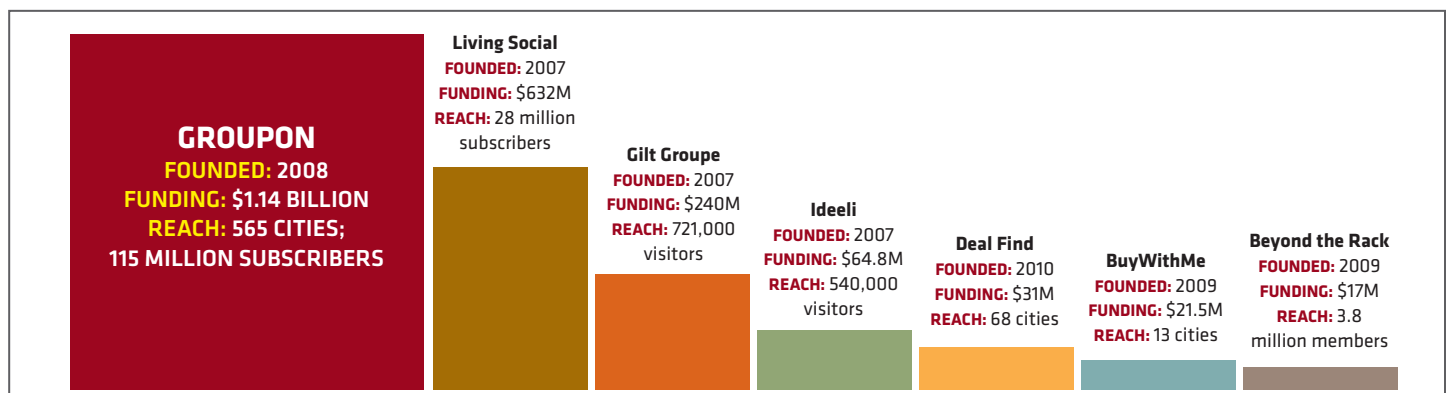
The court’s analysis of the assignment, viewed in light of the SAA, proved decisive in this case. Considering the nature of the rights held by Righthaven under the assignment and under the SAA, the court ruled that, given that the assignment did not assign to Righthaven the legal or beneficial ownership of any exclusive right in the subject copyright, Righthaven actually only possessed “the bare right to bring and profit from copyright infringement actions.” The plain and simple effect of the SAA, it added, was to prevent Righthaven from obtaining, having, or otherwise exercising any right *other than the mere right to sue*, given that Stephens Media *retained* (or was granted back by Righthaven) all other rights and did not itself assign any exclusive right in the applicable copyright to Righthaven.

These rulings, and the fact that Stephens Media could terminate the assignment at any time and effect a complete reversion of the ownership, exposed the assignment as insufficient for the purposes of supporting Righthaven’s standing to sue under the Act, as the EFF had suggested originally. In an order

dated June 14, 2011, the court dismissed with prejudice Righthaven’s suit for lack of standing. In addressing Righthaven’s claim that the SAA did not affect its rights under the assignment – an assertion the court called “disingenuous, if not outright deceitful” – the court ordered Righthaven to show cause why it should not be sanctioned for its failure to disclose Stephens Media as an interested party in this and other Righthaven lawsuits.

The decision in *Democratic Underground* has rippled through other suits brought by Righthaven, as both defendants and presiding judges have taken note of Democratic Underground’s and the EFF’s allegations regarding Righthaven’s standing to sue. One such case is *Righthaven v. Wayne Hoehn*, in which Righthaven sued Hoehn, a registered contributor to madjacksports.com, for copyright infringement based on allegations that he posted an LVRJ article to that site. Hoehn, like the Democratic Underground, challenged Righthaven’s standing to sue on the basis that Righthaven did not own any exclusive right in the article’s copyright. In defending against Hoehn’s assertion, Righthaven and Stephens Media sought to clarify the SAA by entering into evidence an amended version of that agreement, which they argued plainly showed that that the SAA was merely intended to secure Stephens Media’s ability to continue to exploit the subject copyrights following their assignment, and not to limit Righthaven’s right to sue for infringement. Finding Righthaven’s claim (and the amended

## Daily Deals: Who's Who



Sources: <http://www.mofo.com/files/Uploads/Images/111018-MoFo-Tech-Fall-Winter-2011.pdf> (Page 17). Snapshot taken June 2011.

SAA) unpersuasive, the court noted that the amendment did not change the jurisdictional facts as they existed at the time the suit was filed, adding that the original SAA unambiguously qualified later assignments with restrictions and reversionary rights (*i.e.*, an obligation to sue within 60 days, and Stephens Media's right to block any suit) such that, in the end, Righthaven did not actually own any exclusive rights.

The *Hoehn* court ultimately dismissed Righthaven's suit for lack of standing, and Judge Philip Pro held that the amended SAA, even if relevant, had failed to correct Righthaven's standing deficiencies because it still only gave Righthaven an "illusory right" to exploit the copyright. (He also ruled, almost as an aside, that Hoehn's use of the article was protected as fair use regardless of Righthaven's standing to sue.)

Various court orders in a more recent case show that Nevada's appetite for Righthaven's lawsuits may be waning. In *Righthaven v. Pahrump Life*, Righthaven sued a blog owner for allegedly reprinting LVRJ articles. In an order dated August 12, 2011, Judge Mahan reiterated concerns raised in *Democratic Underground* and *Hoehn* concerning Righthaven's standing to sue, supplementing earlier arguments by noting that Righthaven had violated local court rules in failing to list Stephens Media as a party with "a direct, pecuniary interest in the outcome of the case," despite the company's entitlement under the SAA to 50% of Righthaven's recovery. Addressing Righthaven's previous attempts to amend the SAA (and denying Righthaven's request to further amend that agreement), Judge Mahan commented that Righthaven's actions were "merely an attempt . . . to impermissibly change the facts pleaded in the complaint to manufacture standing" and to supplement its complaint with additional facts not present when the case was filed – an impermissible purpose under the Supreme Court's jurisprudence on standing. Although Judge Mahan requested further briefing on Righthaven's standing to sue, the

order made clear that Righthaven would face a steep climb to establish standing and the merits of its claims, and invited Pahrump Life to argue why the case should be dismissed with prejudice.

As more recently reported, Righthaven's standing troubles are not limited to actions filed in Nevada. In an order entered on September 27, 2011 in *Righthaven v. Leland Wolf*, Colorado's Judge John Kane reiterated the holdings of various Nevada courts, including those discussed above, in dismissing Righthaven's copyright infringement suit against a defendant who had reprinted on his personal blog a *Denver Post* photo of a TSA agent performing a pat-down. In holding that Righthaven's "bare right to sue" was insufficient to support its standing to bring suit, Judge Kane added *in dicta* that to allow such suits to proceed would run counter to the constitutional goal of furthering the progress of the arts and the sciences. Specifically, he noted that a party with the bare right to sue "derives its sole economic benefit by instituting claims of infringement, a course of action which necessarily limits public access to the copyrighted work . . . [which] prioritizes economic benefit over public access, in direct contradiction to the constitutionally mandated equilibrium upon which copyright law is based." Some commentators have noted that this Colorado decision may have a domino effect on the other 58 or so cases Righthaven has filed in Colorado, considering that Judge Kane is presiding over all of them.

The fallout from these rulings, which appear to have considerably narrowed Righthaven's room for legal maneuvering, has been dramatic and may signal an end to what some have called Righthaven's "sue-first-ask-questions-later" legal campaign. For example, on August 15, Judge Pro in the *Hoehn* case ruled to award Hoehn over \$34,000 in attorneys' fees and costs, finding the award reasonable and supported by the defendant's arguments. *Wired* later reported that at an early September hearing in which Righthaven indicated its intent to appeal Judge Pro's order, Righthaven told Judge Pro that it might

be forced to seek protection through bankruptcy if the order to pay attorneys' fees was not stayed.

Righthaven has suffered a similar fate in several cases since then. First, following the *Hoehn* ruling, Judge Kane ordered Righthaven to pay the defendant's legal fees. Second, on October 26, 2011, it was reported that Righthaven was ordered to pay \$119,488 in attorneys' fees and costs in the matter of *Righthaven v. Thomas DiBiase* (another Nevada case that was dismissed in light of Righthaven's lack of standing to sue), representing "every dollar [DiBiase's attorneys] asked for in [the defendant's] fee request." And *Ars Technica* recently reported that due to Righthaven's inability to file its appeal on time or pay the over \$34,000 that it was ordered to remit, Judge Pro authorized U.S. Marshals in Nevada to use "reasonable" force to seize nearly \$64,000 in cash and assets from Righthaven, representing the original award plus further costs incurred since August 15, 2011. In the wake of all of these setbacks, it remains to be seen how long Righthaven's litigation campaign will continue to survive.

## Facebook Not "Liked" in Europe, Overhauls Its Privacy Settings

Facebook's "Like" button has been creating problems for Facebook in Europe. Thilo Weichert, the data protection commissioner for the German federal state of Schleswig-Holstein, has told all website owners based in the state to stop using web analytics associated with Facebook, including its "Like" button. "Facebook builds a broad individual and for members even a personal profile. Such a profiling infringes German and European data protection law. There is no sufficient [informing] of users and there is no choice," reads the August 19, 2011 press release (English language version here) from the Schleswig-Holstein

Commissioner. Website owners had until the end of September 2011 to discontinue the use of such analytics.

According to both the German Federal Data Protection Act and the Telemedia Act (German language version here), an individual must give his or her prior informed and explicit “opt-in” consent to the collection and transfer – including online transfers – of his or her data. In addition, individuals must be explicitly informed about their right to withdraw such consent at any point in time.

In November 2009, the Düsseldorfer Kreis, the consortium of German federal data protection authorities, published an Opinion stating that the use of web analytics is only legal where either prior opt-in consent has been obtained or IP addresses have been truncated. A number of EU Member States have also interpreted the recently amended European ePrivacy Directive as requiring informed and explicit (opt-in) user consent prior to the use of web analytics. But to date, Germany has not made any changes to its national legislation, because of existing provisions in the German Telemedia Act.

Commissioner Weichert is also conducting a wider investigation into Facebook’s privacy practices, citing the transfer of user data to the U.S. and the building of profiles without users’ consent or knowledge as infringing data protection laws. The action is a sideways swipe at the social networking service, aimed not directly at Facebook, but at other website owners. Weichert has warned that those website owners cannot “shift their responsibility for data privacy upon the enterprise Facebook . . . and also not upon the users.” Weichert also has expressed concern that Facebook’s offerings are “paid with the data of the users,” sometimes provided unwittingly via other websites. (He has also stated that Facebook fails to meet requirements for providing clear information to users in either privacy notices or its general terms and conditions.)

According to Commissioner Weichert’s recent November 5 press release, enforcement proceedings have been initiated against several undisclosed private and public sector operators for failure to remove and disable their Facebook fan pages, which allow users to show support for a service or product. The Commissioner stated that Facebook ought to amend its consent mechanism and also ensure that no data, including tracking data, are collected from nonmembers. The Commissioner also asked website operators to remove the “Like” button from their websites, according to the statement.

## Facebook’s “Like” button has been creating problems for Facebook in Europe.

The press release stated that in August of this year, Commissioner Weichert had addressed fifteen organizations, including seven public sector and eight private sector entities, asking them to disable their Facebook fan pages and remove the “Like” button, and that so far, only three public sector and three private sector entities have responded to such request in writing and only a single entity – a public sector entity – has complied with the request. Weichert stated that the entities that failed to respond committed a “statutory violation,” because they have an obligation under German data protection law to provide information to the Commissioner when asked to do so. As a result, the Commissioner has issued injunctions against three private companies and threatened them with €5,000 fines if they do not respond and comply with the request.

Under German law, these private sector entities have one month from their receipt of the injunction to object, and can initiate court proceedings to challenge the injunction. Failure to comply may result in a fee of €5,000. The Commissioner also

initiated proceedings against the non-compliant public sector organizations, including ministries of the state of Schleswig-Holstein. And ultimately, website owners could face administrative proceedings and fines of up to €50,000 under Germany’s Telemedia Act.

Edgar Wagner, data protection commissioner for the German federal state of Rhineland-Pfalz, published a statement supporting Weichert and encouraging Facebook and websites to conform to data protection requirements. Wagner pointed to other privacy issues, including that Facebook “undermines the statutory protection of minors.”

Facebook is also being scrutinized elsewhere in Germany: Hamburg data protection commissioner Johannes Caspar has called on Facebook to “delete the stored biometric data of users it collects from its facial recognition software,” which the social networking site has been rolling out in an update of its Tag Suggestions feature. When a user uploads a photograph to his or her profile, the new feature uses facial recognition software to suggest names of people in the photo who can be “tagged,” which causes the photo to be accompanied by a link to the tagged person’s Facebook profile. The suggestions are based on other photos in which those individuals have been tagged. Part of the problem for the Hamburg data protection commission seems to be that the Tag Suggestions feature is enabled by default. The Article 29 Working Party – Europe’s consortium of data protection authorities – is also examining the legality of this feature.

Meanwhile, Europe v. Facebook, an Austrian lobbying group founded by law student Max Schrems, has filed over 20 complaints against Facebook Ireland Ltd., the social networking site’s European headquarters, for a variety of issues including transparency, retention of user data, profiling, and the aforementioned Tag Suggestions feature. The office of the Irish Data Protection Commissioner has confirmed that it will conduct a “comprehensive audit” of



Facebook's Ireland operations amidst these complaints. Part of the audit will involve visits to Facebook's Dublin offices, which a spokeswoman for the Data Protection Commissioner said will "take a number of days." Officials expect to be finished with the audit by the end of 2011. "Facebook is cooperating fully with the audit and we would anticipate that it will implement any necessary changes to comply with any requirements identified," she said.

It is worth noting that Facebook has recently overhauled its privacy settings. In a proactive move, the leading social networking site has updated its privacy settings and controls in an effort to make them easier for users to understand and to give users more control. The new functions include an option for users to view their profiles as their Facebook friends or other users would see them. Facebook users also now have more control over the "Tag" function: they can accept or reject being Tagged by Facebook friends in photos or videos, and can even hold all Tags for approval. On the other hand, the Tag function has been expanded so that a user can be Tagged by any other Facebook user – not just the user's Facebook friends.

## Ninth Circuit Follows *eBay v. MercExchange* and Second Circuit on Preliminary Injunctions for Alleged Copyright Infringement

In its recent opinion in *Perfect 10, Inc. v. Google, Inc.*, the Ninth Circuit Court of Appeals upheld a district court ruling that a copyright infringement plaintiff's showing of likely success on the merits is not in itself sufficient to warrant injunctive relief, particularly absent the

plaintiff's separate demonstration that it will suffer irreparable harm.

The case – the latest skirmish in the long-running battle between Perfect 10 and Google – involved Google's process for complying with Section 512 of the Digital Millennium Copyright Act ("DMCA"). In order to take advantage of the safe harbor protections in Section 512(c) of the DMCA, an online service provider must designate an agent to receive notifications of claimed infringement (so-called "takedown notices"), and make publicly available "substantially . . . the name, address, phone number, and electronic mail address" of such agent. When the online service provider receives an effective takedown notice, the service provider is required to "respond[] expeditiously to remove, or disable access to" the allegedly infringing material.

When Perfect 10 found that Google image searches turned up thumbnail images of Perfect 10's copyrighted photographs of nude models, Perfect 10 sent various DMCA takedown notices to Google, and – given that Google's DMCA policies required (as they still do) that all takedown notices include URLs specifically identifying the allegedly infringing material – Perfect 10's notices included the URLs of the allegedly infringing images that were accessible through Google searches.

Upon receiving the takedown notices, and irrespective of whether Google removed the offending URLs from its search results, Google forwarded the takedown notices to chillingeffects.org, an online educational project run by the Electronic Frontier Foundation and various law schools. This appears to be Google's current policy as well: "Please note that a copy of each legal notice we receive is sent to a third-party which may publish and annotate it (with your personal information removed). As such, the content submitted in this form will be forwarded to Chilling Effects for publication. You can see an example of such a publication at chillingeffects.org.

**The Ninth Circuit's severing of the automatic link between likelihood of success on the merits and irreparable harm could lead to fewer preliminary injunctions in copyright infringement cases.**

For products like Google Web Search, a link to your published notice will be displayed in Google's search results in place of the removed content." When Perfect 10's takedown notices appeared on chillingeffects.org, the allegedly infringing URLs were included in those notices and remained accessible to the general public.

In its suit, Perfect 10 moved for preliminary injunctive relief, alleging that, irrespective of Google's ability to avail itself of the DMCA's safe harbors, the foregoing practice and other practices constituted continuing infringement by Google of Perfect 10's copyright in its photographs. But the district court denied Perfect 10's motion for an injunction, holding that Perfect 10 failed to demonstrate that it was likely to suffer irreparable harm without preliminary injunctive relief being granted – one of the four traditional criteria for granting preliminary injunctive relief.

On appeal, Perfect 10 cited Apple Computer, Inc. v. Formula International, Inc., which states that "[a] showing of reasonable likelihood of success on the merits in a copyright infringement claim raises a presumption of irreparable harm" that can lead a court to issue a preliminary injunction. The Ninth Circuit, however, affirmed the district court's ruling, citing both the more recent eBay Inc. v. MercExchange,

*L.L.C.* decision, in which the United States Supreme Court held that language in the Patent Act did not require injunctive relief whenever there was patent infringement, and *Salinger v. Colting*, a Second Circuit case that extended the *eBay* decision to copyright cases, doing away with the presumption that “a plaintiff likely to prevail on the merits of a copyright claim is also likely to suffer irreparable harm” without being granted a preliminary injunction.

In agreeing with the Second Circuit, the Ninth Circuit noted that the Copyright Act did not indicate any congressional intent “to authorize a major departure from the traditional four-factor framework that governs the award of injunctive relief[.]” The Ninth Circuit therefore held that Perfect 10’s showing of likely success on the merits was not in itself sufficient to create a presumption of irreparable harm, and Perfect 10’s failure to establish that it had suffered irreparable harm from Google’s actions required a denial of the plaintiff’s motion for a preliminary injunction.

Although it may be too early to predict the ramifications of this latest Perfect 10 ruling, the Ninth Circuit’s reinforcement of the traditional four-factor preliminary injunction test as applied to copyright holders – and its severing of the automatic link between likelihood of success on the merits and irreparable harm – could lead to fewer preliminary injunctions in copyright infringement cases, or perhaps fewer copyright infringement suits being filed in situations where irreparable harm is difficult to demonstrate. Some have [opined](#) that it will now become much harder to convince a court of irreparable harm when there is a more tangential infringing use of copyrighted material, for example, “artwork on a wall in the background” of a film. Further, by focusing on the requirements for a preliminary injunction, the Ninth Circuit avoided having to answer one of the more interesting questions, that is, whether posting URLs to allegedly infringing materials on

chillingeffects.org (or similar sites) itself constitutes copyright infringement.

## The FTC Proposes Changes to Its COPPA Rule – And Why Every Website Operator Should Pay Attention

The Federal Trade Commission (“FTC”) recently released [proposed amendments](#) to its rule (“Rule”) implementing the Children’s Online Privacy Protection Act (“COPPA”). The Rule requires the operator of a website or online service to obtain verifiable parental consent before collecting personal information from a child under the age of 13. If adopted as drafted, the revised Rule would not only make it even more difficult for operators to collect information from children online, but it would also sweep into the Rule’s coverage sites and online services that are currently outside of it. Moreover, the proposed changes would codify the erasure of the traditional distinctions between “personal” and “non-personal” information – an outcome that raises issues even for companies that are not subject to COPPA.

Among the most significant changes proposed by the FTC are the elimination of the widely used “email plus” method of obtaining verifiable parental consent and a considerable expansion of the Rule’s definition of “personal information.”

**Elimination of the “email plus” method of obtaining consent.** The existing Rule has a two-tiered system for obtaining verifiable parental consent: An operator that uses a child’s information only internally may use the so-called “email plus” mechanism, while more foolproof measures, such as a print, sign, and send back form or a phone call, are required if the operator will disclose the child’s information to third parties. Asserting that “all collections of children’s information

**The FTC’s proposals reflect its oft-stated position that the line between what has traditionally been considered “personal” and “non-personal” information is increasingly blurred, such that protections historically afforded to personal information should be extended to certain non-personal information as well.**

merit strong verifiable parental consent,” the FTC has proposed to eliminate the distinction. “Email plus” – currently the most common way of obtaining consent – would no longer be an option.

**Expansion of the definition of “personal information.”** At the same time that it proposes to make obtaining verifiable parental consent more difficult and costly, the FTC also proposes to extend the Rule’s reach to a far wider swath of information collection practices, by expanding its definition of “personal information.” Perhaps most notably, the FTC would include within the definition a persistent identifier, *when it is used for functions other than support for the internal operations of the site or service.* “Persistent identifiers” include a customer number held in a cookie, an IP address, a device serial number, and a unique device identifier. In its commentary accompanying the proposed revisions, the FTC explains that consent would not be required when persistent identifiers are used for purposes such as user authentication, improving navigation, maintaining user preferences, serving contextual advertising, and protecting against fraud or theft, as these are functions that support the internal

operations of the site or service.

On the other hand, the “personal information” definition would be triggered by – and verifiable parental consent would therefore be required for – other, non-support uses, presumably including online profiling, the delivery of personalized content, behavioral advertising, retargeting, and analytics. This is significant because there is no way to determine age from a persistent identifier – meaning, for instance, that sites directed to children could not deliver personalized content without first obtaining verifiable parental consent. For sites not directed to children but that are still subject to the Rule (because they knowingly collect personal information

from children under 13), it is not clear how this restriction would apply in practice. As companies facing similar consent requirements in the EU can attest, obtaining consent prior to the use of a persistent identifier can be a costly and disruptive obligation. The FTC does not provide guidance in its commentary, but the issues are ripe for comment.

The FTC’s proposals reflect its oft-stated position that the line between what has traditionally been considered “personal” and “non-personal” information is increasingly blurred, such that protections historically afforded to personal information should be extended to certain non-personal information as well. If the FTC takes this approach with

respect to COPPA, it is logical that it will take a similar approach in all contexts. Therefore, even companies not subject to COPPA are advised to consider the potential ramifications of the proposed changes and to consider submitting comments. The FTC is accepting comments until December 23, 2011.

---

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

---

## About Morrison & Foerster

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, *Fortune* 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last 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

In the latest chapter of an [ongoing](#) dispute, Judge Marvin E. Aspen of the U.S. District Court for the Northern District of Illinois was [not hot](#) for Teachbook.com's motion to dismiss Facebook's trademark infringement action. The court denied the motion, holding that the suffix "book" was not necessarily generic as used by Facebook in connection with social networking services.

Continuing with the trademark segment of our program, Twitter [announced](#) that it has settled a trademark dispute with one of its app developers regarding the developer's registration for the slogan "Let Your Ad Meet Tweets," which had been blocking Twitter's own application to register its "tweet" mark.

Bad news travels fast: An Australian social media monitoring firm [estimated](#) that Twitter hit 10,000 tweets per second following news of Steve Jobs' death, beating the previous record of 8,868 tweets per second set when Beyonce announced her pregnancy at the MTV Video Music Awards.

Proving once again that old chestnut about an ounce of prevention, the Bank of Melbourne recently had its Twitter account [hijacked](#), reportedly due to a weak Twitter password used by an employee. The hijacker then used the bank's account to send phishing messages to followers, including the bank's customers.

Facebook was hit with a [class action complaint](#) based on allegations that its use of cookies to collect information on users even when they were logged out of the Facebook site violates the federal Wiretap Act and various Kansas state laws. The Kansas action follows a [similar suit](#) in California, as well as complaints from privacy groups. And more recently, [German regulators](#) have been looking into the issue. For its part, Facebook has [denied](#) that it tracks users' Internet activity.

Wrapping up our Facebook privacy coverage (and what social media report is complete without a good-sized helping?), German researchers were reportedly able to steal 250GB of

personal information from Facebook by using fake profiles and "a virtual army" of bots. Demonstrating a keen understanding of human nature, the researchers gave the bots photos of attractive individuals from the "Hot or Not" website to raise the chances of successful friending. If you are concerned that some of your Facebook friends may be bots, we suggest a [series of probing questions](#) to root out the imposters.

British Columbia's Information and Privacy Commissioner has issued [new guidelines](#) to assist organizations and public bodies using social media sites to conduct background checks of prospective employees, volunteers, and candidates.

Buzz kill: Google [announced](#) that it is discontinuing Google Buzz in order to concentrate its social media efforts on its newer Google+ service. Google Buzz was the source of various problems for the search giant, including a class action lawsuit and FTC investigation regarding privacy complaints. Continuing with its spring cleaning, Google also [announced](#) that it is discontinuing its Sidewiki website annotation tool.

No Facebook friends? Your brain's to blame: [Research suggests](#) that the number of Facebook friends you have may correlate with the size of certain regions of the brain.

We have a certain fascination with social media stats here at *Socially Aware*, so we were interested to see that a data analytics company [reported](#) that Google+ traffic spiked 1,200% soon after launching, but has since fallen by 60%. *Sic transit gloria mundi*, as they used to say back in the old neighborhood.

Marking humankind's latest triumph, the .com top-level domain is [closing in](#) on 100 million registered domain names. We should all be very proud.

More fun with numbers: LinkedIn CEO Jeff Weiner [told listeners](#) on an earnings call that the professional social network now has 131 million members and more than a million groups. More than 15 million people joined LinkedIn in the third

quarter of 2011, representing a 63% increase over the growth rate from the same period last year.

Is that a real job? The NLRB recently [decided](#) against a law firm technology employee who was fired when he listed his job title as "f\*\*\*\*ard" on LinkedIn. (Note: This item has been sanitized for your protection.) The Board determined that the worker had failed to support his claim that the termination actually resulted from his overtime policy discussions with co-workers.

In the most recent ruling in *Levitt v. Yelp!* (a case we have [covered](#) previously), the U.S. District Court for the Northern District of California held that the Communication Decency Act's protections do not depend on the service provider's motive for editing user submissions. Quoting the Ninth Circuit's folksy waterfowl metaphor from the *Roommates.com* case, the court noted that, from a policy perspective, linking immunity under the Communication Decency Act to a service provider's motives could result in "death by a thousand duck-bites."

Most expensive tweet ever? [Reports](#) are that the NBA fined Miami Heat owner Micky Arison \$500,000 for tweeting about the NBA lockout in response to a tweet from a fan.

We've given up trying to get through an issue of *Socially Aware* without mentioning teen pop sensation Justin Bieber. The singer recently became the first person ever to have over [two billion official You Tube views](#).

As we have [previously reported](#), Facebook has aggressively pursued spammers who target Facebook users. Facebook racked up a win in one of its anti-spam lawsuits when the U.S. District Court for the Northern District of California [held](#) that the social media giant sufficiently pleaded claims under the CAN-SPAM Act and the Computer Fraud and Abuse Act, as well as common law fraud, against Internet marketing company Max Bounty.