

Socially Aware: The Social Media Law Update

2011 Best Law Firm
Newsletter



In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we examine why social media marketing strategies should be concerned with clearing more than just copyrights; we revisit how affirmative user consent can make all the difference when it comes to the enforceability of your terms of use agreement; we review the FTC's guide to mobile application development, which outlines practices that mobile app developers should follow to avoid Section 5 enforcement against unfair or deceptive acts or practices; we discuss measures that companies collecting personal information from California residents can take to help ensure compliance with California's Online Privacy Protection Act (OPPA); we report on California's latest legislative efforts to restrict employers' access to employees' and applicants' personal social media accounts; we fill you in on an important Seventh Circuit contributory copyright infringement case; we take a look at a complaint against a leading web-based print-on-demand service that demonstrates how social media and similar sites can become easy targets for trademark infringement claims; we highlight a recent FTC settlement with a well-known data broker that implicates both the Fair Credit Reporting Act (FCRA) and the FTC's Endorsement Guides; and we provide an update on the controversy as to whether "liking" something on a social media site amounts to constitutionally protected speech.

All this, plus a collection of thought-provoking statistics on the use of social media during the recent 2012 presidential election.

Follow us on Twitter [@MoFoSocMedia](#), and check out our [blog](#).

IN THIS ISSUE

- 2** The Potential Perils of Posting Pictures (on Social Media)
- 3** That's a Wrap: *Nguyen v. Barnes & Noble*
- 5** FTC Issues Guidance for Mobile App Privacy and Advertising; Signals More Enforcement Coming
- 6** California A.G. Targets Mobile Apps That Fail to Comply With the State's Privacy Policy Law
- 7** New California Law Limits Employer Access to Employee Social Media Accounts
- 7** Judge Posner Kicks That Flava in Ya Ear: New Guidance on Contributory Infringement From the Seventh Circuit
- 9** Born to Mock: Trademark Holder's Fight to Remove Mark on Kitsch Merchandise May Have Broad Legal Implications
- 10** The FTC's Spokeo Settlement Highlights Social Media-Related Legal Risks
- 11** Update: What's Not to Like?

EDITORS

John Delaney
Gabriel Meister
Aaron Rubin

CONTRIBUTORS

Nicholas Datlowe
Anna Ferrari
Reed Freeman
Matthew Galeotti
Timothy Denny Greene
Jacob Michael Kaufman
Christine Lyon
Julie O'Neill
Debbie Rosenbaum
Nathan Salminen
Jesse Soslow

The Potential Perils of Posting Pictures (on Social Media)

In today's information economy, content owners are faced with a challenging decision regarding digital content. On the one hand, the viral nature of social media can lead to unprecedented exposure as digital content is shared. On the other, that same opportunity carries with it significant legal risk if companies take an insufficiently careful approach to intellectual property clearance issues. One luxury clothing brand, Burberry Ltd., recently discovered just how substantial that legal risk can be.

Burberry approached social media with an innovative concept: "historical timelines" on its various social media pages, including [Facebook](#), [Twitter](#), and [Instagram](#). These timelines featured photos of celebrities wearing Burberry's iconic trench coats, scarves, and other products. Among Burberry's chosen photos was a shot of Humphrey Bogart from the final scene of [Casablanca](#), in which Bogart's Rick, clad in a timeless Burberry trench, sends Ingrid Bergman's Ilsa off to Brazzaville. And although Burberry acquired permission to use the photo from photo agency [Corbis](#), which manages the rights to various stock photos from [Casablanca](#), Burberry failed to clear its use with [Bogart LLC](#), which owns the actor's publicity rights.

Applicable law allows a celebrity to object to use of his or her name or likeness in a commercial context, particularly if the use is likely to cause members of the intended market to believe that the celebrity endorses the product. Bogart LLC alleged that Burberry's use of the photo falsely implied that Bogart had endorsed the brand, thereby violating Bogart LLC's publicity rights. Burberry countered, arguing that its timelines constituted "a historical positioning of the image within an educational project along with

numerous other photographs of people wearing Burberry apparel over the last century."

Although Burberry and Bogart LLC settled their pending state and federal cases for an undisclosed amount, this case provides a good example of the unexpected issues that can arise when brand managers fail to consider the full spectrum of rights that may be implicated by the use of photographs and other content. While the content industries have spent the last decade educating the public on *copyright law's* effects in the digital media world, less attention has been paid to other areas of potential liability, such as trademark infringement and privacy and publicity rights violations, and their respective effects on the social media experience.

The viral nature of social media can carry significant legal risk if companies take an insufficiently careful approach to IP clearance issues.

For example, in 2007, Virgin Mobile Australia (VMA) launched an advertising campaign using amateur photography culled from the social photo-sharing site, [Flickr](#). The photos used by VMA were licensed under a Creative Commons "Attribution" license, which requires only that the original creator—that is, the copyright holder—be given credit. VMA chose for its campaign a photo of then-15-year-old Alison Chang, taken by her church youth counselor and uploaded by him to Flickr. Although VMA had appropriate copyright clearance to use the counselor's picture under the Creative Commons license, Chang's parents sued VMA for failing to get permission from Chang or her parents to use Chang's name or likeness. Although the case was dismissed on procedural grounds, the incident illustrates how

easily (and often) clearance procedures are overlooked when it comes to Internet-based content.

Similar cases have raised complex issues relating to federal preemption of state law claims. For example, in [Laws v. Sony Music Entertainment, Inc.](#), the plaintiff sued Jennifer Lopez and LL Cool J, alleging misappropriation of her name and voice through use of a sound recording on which the plaintiff's voice was featured. The defendants had obtained a license to use the sound recording on which the plaintiff's voice was featured, but had not obtained from the plaintiff the right to use her voice. Nonetheless, the Ninth Circuit held that, on this set of facts, the federal Copyright Act preempted the plaintiff's state law right-of-publicity claim. Thus, her permission was not required for the defendants to use the validly licensed sound recording. By contrast, a different Ninth Circuit panel, in [Downing v. Abercrombie & Fitch, Inc.](#), held that the Copyright Act did *not* preempt the plaintiffs' state law publicity claims based on Abercrombie's advertising use of a photo of the plaintiffs taken after the 1965 Makaha International Surf Championship in Hawaii. Thus, Abercrombie should have sought the plaintiffs' permission in the first instance. The preemption inquiry is fact-bound—the Copyright Act preempts state law publicity claims in some circumstances, but not others.

Although the details of these preemption cases exceed the scope of this article, suffice it to say that a company's social media marketing personnel may not have the expertise to wade through such complex clearance issues. A clearance system that focuses narrowly on copyright issues and doesn't consider other forms of intellectual property may therefore invite unexpected claims. It is also worth noting, as we note elsewhere in this issue, that the safe harbors provided by the [Digital Millennium Copyright Act](#) (DMCA) apply only to copyright claims, not other types of claims such as those mentioned above—

and in any event, such safe harbors provide protection only with respect to user-generated content, not content posted by a company's own employees. Therefore, companies should not assume that the DMCA will shield them from all liability for content posted on their social media pages.


Social media is an exciting new channel for reaching both current and prospective customers. But from a rights-clearance perspective, the old rules largely remain in force. Accordingly, companies' review procedures for company-driven social media content should, to the extent possible, mirror the process they undertake for print ads and other traditional media. And where that may not be feasible (given the speed and flexibility often required on social media platforms), companies should institute rigorous policies and train marketing associates on how to avoid potential liability.

That's a Wrap: Nguyen v. Barnes & Noble


Website operators often take for granted the enforceability of their websites' terms of service. In a recent order issued in a case from the Central District of California, Nguyen v. Barnes & Noble, Inc., Judge Josephine Tucker reminds us that such presumptions are not necessarily correct: terms of service that do not require an affirmative manifestation of assent from a website user may not always be upheld in court.

Many website operators, particularly Internet retailers and operators of ecommerce sites, use "clickwrap" (or "clickthrough") agreements to govern the use of their sites. With clickwrap agreements, the website operator typically presents its standard terms of use and then requires the user to click an "Accept" or "I Agree" button. By clicking the button, users affirmatively manifest their intent to be bound by the terms. Other website operators use


SOCIAL MEDIA STATS: 2012 ELECTION




With over **20 million tweets**, Election Day 2012 was the most tweeted-about event in U.S. political history. **1**




The election's most tweeted moment followed the projection of Obama's reelection, generating over **327,000 tweets per minute**. **2**




U.S. Facebook users mentioned Election Day-related topics **71.7 million times** on November 6, making it the most talked-about topic on Facebook in the United States this year. **3**




Facebook disclosed that Election Day mentions of "**Obama**" in the six hours between 3 PM ET and 9 PM ET were **43 percent higher** than mentions of "**Romney**." **4**



The Obama campaign's victory tweet of a **photo** of the President hugging the First Lady, with the words "**Four More Years**," became Twitter's **most re-tweeted post of all time** in less than one hour. **5**



The same victory **photo** was also the **most "Liked" photo of all time** on Facebook. **6**



Over **one in five** registered voters used social media to let others know that they voted. **7**

1. https://twitter.com/gov/statuses/266016146204000256?tw_i=266016146204000256&tw_e=permalink&tw_p=tw

2. https://twitter.com/gov/statuses/266043982021292032?tw_i=266043982021292032&tw_e=details&tw_p=tw

3. <http://mashable.com/2012/11/08/election-day-facebook/>

4. <http://www.digitaltrends.com/social-media/election-night-2012-by-the-social-media-numbers/>

5. <http://www.digitaltrends.com/social-media/election-night-2012-by-the-social-media-numbers/>

6. <http://mashable.com/2012/11/07/obama-most-liked-facebook/>

7. <http://pewresearch.org/pubs/2414/social-media-networks-politics-voting-voters-discussing-vote-encouraging-voting>

"browsewrap" agreements—terms of use agreements that are usually accessible through a hyperlink at the bottom of a web page. Although, as a practical matter, few people actually read browsewraps, they are widely used.

Both clickwraps and browsewraps are

contracts of adhesion in legal parlance. That is, they are contracts that are offered on a "take it or leave it" basis with no opportunity for negotiation. A user who does not wish to be bound by the proffered terms can click "Do Not Accept" or, for a browsewrap, simply leave the website. On the other hand, a user who is willing to be bound can indicate

such assent by clicking “I Accept” or by continuing to browse the website.

Reasonable people may disagree regarding whether these actions truly manifest a user’s assent to be bound by the relevant contract terms, but courts have frequently upheld the enforceability of both clickwrap and browsewrap terms of use (subject, of course, to the unconscionability concerns raised by any contract of adhesion). As discussed below, however, browsewrap terms of use often encounter a greater degree of scrutiny from courts due to the lack of any affirmative acceptance by users.

The enforceability of browsewrap terms of use has been held to depend on whether a website user has knowledge—either actual or constructive—of the applicable terms, because users cannot agree to be bound by terms unless they know what those terms are. Courts considering browsewrap enforceability issues often grapple with the question of whether the defendant was given notice of the applicable terms sufficient to impute such knowledge. For example, in *Register.com, Inc. v. Verio, Inc.*, the court determined that numerous and repeated queries by an automated software program were sufficient to show that Verio knew of, and was bound by, Register.com’s terms (although Verio had also admitted that it had actual knowledge of the terms). On the other hand, in *Ticketmaster Corp. v. Tickets.com, Inc.* the court held that a small terms of use link that was visible only if the user scrolled down to the bottom of the web page was insufficient to establish notice. But, three years later, the same court (in the same case, no less) ruled that more prominent notice on the site’s home page was adequate notice. While a court’s determination of sufficient notice may vary in each case, it is clear that the more readily available and conspicuous browsewrap terms of use are, the more likely it is that a court will find that the user knew of, and was bound by, such terms.

That brings us to *Nguyen v. Barnes & Noble, Inc.* In *Nguyen*, the plaintiff’s

claims arose from a Barnes & Noble promotion that offered computer tablets at a discounted price. Although Nguyen submitted an order to purchase a tablet at the promotional price, Barnes & Noble canceled his order the next day, citing an oversale of its tablet inventory. As a result, Nguyen alleged that he was “forced to rely on substitute tablet technology, which he subsequently purchased . . . [at] considerable expense.” In April 2012, Nguyen filed suit, alleging various consumer protection violations, including false advertising, unfair competition, and breach of contract, under California and New York law. Barnes & Noble then moved to compel arbitration based on an arbitration clause included in its website’s browsewrap terms of use. The question before the court was whether, given the existing facts, the arbitration clause was enforceable against Nguyen.

A simple click can mean the difference between whether or not a terms of use agreement is found to be enforceable.

The court ultimately held that the arbitration clause was not enforceable because the terms of use agreement itself was not enforceable. According to Judge Tucker, Barnes & Noble’s website terms of use could not bind Nguyen because Barnes & Noble “did not position any notice even of the *existence* of its ‘Terms of Use’ in a location where website users would necessarily see it, and certainly did not give notice that those Terms of Use applied, except within the Terms of Use” (emphasis in original). Due to this lack of adequate notice, Nguyen did not know and, in Judge Tucker’s view, should not necessarily have known of Barnes & Noble’s terms of use. Because Nguyen did not have knowledge of the terms, he could not be bound by them. Therefore,

Barnes & Noble could not compel arbitration in its dispute with Nguyen.

In light of *Nguyen* and the other cases discussed above, website operators should consider using clickwraps that require affirmative acceptance where possible, rather than relying on browsewraps to enforce their terms of use. A simple click can mean the difference between an agreement’s being found enforceable or not. For ecommerce sites or any site that requires registration prior to use, clickwraps are relatively easy to implement—for example, at the point of purchase or when the user registers—without negatively affecting the user experience. Best practices for clickwraps include presenting terms of service before payment, allowing for easy reading of all terms, allowing users to print or save a copy of the terms, offering a prominent option to decline the terms, providing an easy way for users to find the terms on the site at any time after payment or registration, and giving users notice of (and requiring users to accept) any updates and changes to the terms of use.

For other sites, including some social media sites, the story may differ. Many social media sites—for example, [Pinterest](#), [Twitter](#), and [YouTube](#)—allow users to access at least some content and functionality without registering. With sites such as these, there may be no real opportunity to obtain affirmative acceptance of terms of use without degrading the user experience, so a clickwrap is simply not a practical option. For operators of such websites, the most important lesson of *Nguyen* and the other cases discussed above is that the question of enforceability often turns on whether the user has sufficient notice of the terms of use. Therefore, website operators can increase the likelihood that their terms of use will be enforced if links to those terms are prominently displayed, preferably “above the fold” so that a user will be able to see the link without scrolling down the page. As *Nguyen* and the other cases illustrate, an operator who places its terms of use link in a tiny font buried at the bottom of a page may be in for an unpleasant surprise if those terms ever need to be enforced.

FTC Issues Guidance for Mobile App Privacy and Advertising; Signals More Enforcement Coming

On September 5, 2012, the Federal Trade Commission (FTC) published a brief guide to assist developers of mobile applications, both large and small, in complying with truth-in-advertising, privacy, and data security principles. In publishing this advice, the FTC makes clear that its [Section 5](#) enforcement powers against unfair or deceptive acts or practices apply in the mobile app arena, and with equal force to large and small developers.

The FTC's guidance briefly lays out the practices developers should follow in order to avoid such enforcement, thereby suggesting that more enforcement is on the horizon. Indeed, it has already started: in August 2011, the [FTC reached a settlement](#) with W3 Innovations, LLC for alleged violations of the COPPA rule in its apps directed at children.

The guide, called "[Marketing Your Mobile App: Get it Right from the Start](#)," explains general consumer protection principles, and applies them to the context of mobile applications. Although the title of the guide suggests that the advice is primarily about marketing the apps, the FTC also gives advice about the design and implementation of apps.

What Is This Guide?

This is NOT a new FTC trade regulation carrying the force of law. This is guidance issued by the Commission for how it may apply its Section 5 authority to police deceptive and unfair practices in the app environment. The FTC expects that the

industry will review this guidance and take it into account in developing and advertising their apps.

This guidance is also specifically directed at mobile app developers; it does not relate to the "[In Short](#)" [Dot-Com Disclosures](#) workshop held on May 30, 2012, which relates to proper disclosure techniques in all online commerce. Guidance arising from that workshop, which is expected to be far more fulsome, is anticipated to be released by the end of 2012.

The FTC's guide briefly lays out the practices that mobile app developers should follow to avoid Section 5 enforcement against unfair or deceptive acts or practices.

What Compliance Steps Is the FTC Looking For?

Substantiate Your Claims

The FTC advises that app developers advertise their apps truthfully, and explains that "pretty much anything" a company tells a prospective user about what the app can do, expressly or by implication, no matter the context, is an "advertisement" requiring substantiation for claims as they would be interpreted by the average user.

If Disclosures Are Necessary, Make Them Clearly and Conspicuously

If developers need to make disclosures to users in order to make their advertising claims accurate, the FTC notes, then those disclosures must be clear and conspicuous. Although this

does not require specific type or font sizes, the disclosures must be large enough and clear enough that users both see and understand them. This means, according to the FTC, that disclosures cannot be buried behind vague links or in blocks of dense legal prose.

Incorporate Principles of "Privacy by Design" in Developing Apps

The FTC also gives advice to developers on how to avoid enforcement for violations of user privacy. First, it notes that developers should implement "privacy by design," meaning that they should consider privacy implications from the beginning of the development process. This entails several elements:

- Incorporating privacy protections into your practices;
- Limiting information collection;
- Securely storing held information;
- Disposing of information that is no longer needed;
- Making default privacy settings consistent with user expectations; and
- Obtaining express user agreement for information collection and sharing that is not apparent.

Incorporate Transparency and Choice Into Apps and Honor Users' Choices

The FTC urges that developers be transparent about their data collection practices, informing users about what information the app collects and with whom that information is shared. Developers should also, according to the FTC, give users choices about what data the app collects, via opt-outs or privacy settings, and give users tools that are easy to locate and use to implement the choices they make.

Importantly, the FTC emphasizes that developers must honor the choices they

offer consumers. This includes following through on privacy promises made. This also includes getting affirmative permission from users for material changes to privacy practices—simply editing the privacy policy is not enough, according to the FTC guide.

Apply COPPA Protections Where Appropriate

The FTC notes that there are special rules for dealing with kids' information. Developers who aim their apps at children under 13, or know that children under 13 are using the app, must clearly explain their information practices and obtain verifiable parental consent before collecting personal information from children. The guide links to further advice for compliance with the Children's Online Privacy Protection Act (COPPA).

Special Protections for Sensitive Information

Even for adults, the FTC urges developers to get affirmative consent before collecting "sensitive" information, such as medical, financial, or precise location information. For sensitive information, the FTC states that developers must take reasonable steps to ensure that it remains secure. The FTC suggests that developers:

- Collect only the information needed;
- Take reasonable precautions against well-known security risks;
- Limit access to the data to a need-to-know basis; and
- Dispose of data safely when it is no longer needed.

The FTC notes that these principles apply to all information the app collects, whether actively from the user, or passively in the background. In addition, any contractors that work with the developers should observe the same high security standards.

California A.G. Targets Mobile Apps That Fail to Comply With the State's Privacy Policy Law

On October 30, 2012, California Attorney General Kamala Harris announced that her office would begin notifying the developers of as many as 100 mobile apps that their apps do not comply with the state's Online Privacy Protection Act (OPPA) and that they have 30 days to bring them into compliance.

Companies that collect personal information online from California residents—whether through a website, online service, or app—should take steps to ensure that they are in compliance with the state's Online Privacy Protection Act (OPPA).

The announcement does not come as a surprise. As reported in our August 2012 issue of *Socially Aware*, the Attorney General published a Joint Statement of Principles with the major platforms that distribute and sell mobile apps, providing that they will distribute only apps that have privacy policies that consumers are able to review prior to download. At that time, her office told app developers that they had six months to come into compliance or to be notified of violations. Shortly thereafter, Attorney General Harris formed a Privacy

Enforcement and Protection Unit, intended specifically to enforce OPPA and other privacy laws.

In light of the Attorney General's announcement and her continued focus on privacy, companies that collect personal information online from California residents—whether through a website, online service, or app—should take steps to ensure that they are in compliance. According to the Attorney General's sample non-compliance letter attached to her press release, failure to comply could subject a company to a fine of up to \$2,500 each time a non-compliant app is downloaded.

The Law's Requirements

OPPA requires a commercial website operator or online service provider, including a mobile app developer, that collects personally identifiable information (PII) from consumers residing in California to post a conspicuous privacy policy. Because OPPA applies to any company that collects data online about California residents, companies both within and outside of California may be subject to enforcement activity.

Under OPPA, the privacy policy must include:

- The categories of PII that the website, online service, or app collects from its users;
- The third parties with whom such PII may be shared;
- The process by which the consumer can review and request changes to his or her PII, if the website operator, online service provider, or app developer maintains such a process;
- The process by which the operator, provider, or developer notifies consumers of material changes to its privacy policy; and
- Its effective date.

Additional Considerations

Compliance with OPPA does not necessarily ensure compliance with all applicable laws. In particular, the Federal Trade Commission (FTC) has long taken the [position](#) that privacy policies should describe, in a way that consumers can easily understand, all material collection, use, and disclosure practices. This means that, in addition to the information required by OPPA, a privacy policy should include other disclosures, such as:

- Its scope;
- How PII may be used;
- How “other information”—information that may not be considered PII but the collection of which may be material to users—is collected, used, and disclosed. This may include, for instance, users’ clickstream information or other information derived from their interaction with the website, service, or app and collected for purposes of personalizing content or displaying targeted ads;
- How PII is secured and for how long it may be retained;
- How the user may exercise various rights, such as the right to opt out of receiving direct marketing or the right to opt out of the sharing of his or her PII with third parties;
- How the user may access the PII collected from him or her and the control that he or she has with respect to such PII; and
- How the user can contact the operator or developer.

Drafting a compliant privacy policy is only the first step. A company must also implement measures to ensure that it complies with the representations it makes in its privacy policy, to avoid claims that its privacy policy is deceptive or misleading.

In light of the increased enforcement activity by the California Attorney General and FTC, mobile app developers

will want to ensure that each mobile app includes a privacy policy, that the privacy policy is conspicuously posted on the mobile app, and that the privacy policy is followed in practice.

New California Law Limits Employer Access to Employee Social Media Accounts

On September 27, 2012, California Governor Jerry Brown signed a bill that restricts employer access to the “personal social media” of employees and applicants for employment.

Assembly Bill 1844 (“AB 1844”) adds to the California Labor Code new section 980. Under this section, an employer may not “require or request” an employee or applicant to do any of the following:

- Disclose a username or password for the purpose of accessing personal social media;
- Access personal social media in the employer’s presence; or
- Divulge any personal social media, except in connection with the investigation of allegations of an employee’s misconduct or violation of applicable laws.

The exception for employee investigations applies if the employer reasonably believes that the personal social media is relevant to the investigation or to a related proceeding, and does not use the personal social media for any other purpose. Further, the bill does not preclude an employer from requiring or requesting an employee “to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device.”

California has joined the growing list of states that restrict employer access to employees’ personal social media.

AB 1844 expressly prohibits retaliation against an employee or applicant who declines to comply with a request that violates the terms of AB 1844, but it does not immunize the individual from any adverse action that is otherwise permitted by law. Notably, the state Labor Commissioner is not required to investigate or determine violations of AB 1844.

AB 1844, which passed in both the California Senate and Assembly by wide margins, is similar to recently enacted laws in Delaware, Maryland, and Illinois. (As we reported in [our June 2012 issue of *Socially Aware*](#), Maryland led the charge by becoming the first state to prohibit employers from requesting employees’ social media passwords.) During this legislative season, at least 13 states have proposed legislation restricting employer access to employee social media accounts, including Massachusetts, Michigan, Minnesota, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington.

Judge Posner Kicks That Flava in Ya Ear: New Guidance on Contributory Infringement From the Seventh Circuit

Over the past year, a number of courts across the country have decided cases involving contributory infringement and

the application of the [Digital Millennium Copyright Act's § 512\(c\) safe harbor](#) in the social media context. Unfortunately for those who favor a uniform approach to the law, the precedent being developed is in many ways inconsistent. On one side of the country, the Ninth Circuit solidified § 512(c)'s protections for social media sites in [UMG Recordings, Inc. v. Shelter Capital Partners LLC](#) by holding that social media sites are not liable for user-posted infringing material, subject to compliance with the DMCA's notice and takedown procedures. Several months later on the other side of the country, the Second Circuit addressed similar questions in [Viacom Int'l, Inc. v. YouTube, Inc.](#) Judge Cabranes's opinion introduced the possibility that a social media site-owner's "willful blindness" to infringing activity may trigger liability, thus raising the specter of (very) expensive litigation. The Seventh Circuit has now held in [Flava Works, Inc. v. Gunter](#) that online service providers are protected from contributory infringement liability—and therefore need not depend on the DMCA's safe harbors at all—where they do not actually host allegedly infringing material or encourage copyright infringement, but merely link to such material.

In an opinion written by one of [the country's preeminent circuit judges](#) and [cat fanciers](#), [Richard Posner](#), the court addressed whether to uphold a preliminary injunction against [social bookmarking](#) site myVidster for [contributory copyright infringement](#). myVidster allows users to "bookmark" videos they find on the Internet, such as videos from [YouTube](#) or [Vimeo](#). myVidster automatically retrieves the "embed code"—code that permits the video to be viewed in a browser window separate from the original website (for example, when you link to a YouTube video on your Facebook page, the site automatically embeds the video so that your friends can view the video on Facebook rather than having to visit YouTube). myVidster then creates a new page for the embedded video, replete with advertisements.

Plaintiff Flava Works is an entertainment company that produces and streams adult videos through various websites. Flava allows its customers to download its content solely for personal use. Users are not permitted to upload Flava's videos to other sites or to create any additional copies of the content. Thus, in Judge Posner's view, a user who copies Flava's videos by downloading them and then uploading the copyright-protected videos to a third-party website is a direct infringer of Flava's copyright. Because myVidster didn't upload the infringing videos, the court found that myVidster did not directly infringe Flava's copyright.

The Seventh Circuit has held that OSPs are protected from contributory infringement liability where they do not actually host allegedly infringing material or encourage copyright infringement, but merely link to such material.

The court next considered whether myVidster should be held liable for contributory infringement based on such copying by Flava's users. Posner disregarded the oft-cited [Gershwin Publishing Corp. v. Columbia Artists Management, Inc.](#) definition of contributory infringement in favor of a more succinct standard from [Matthew Bender & Co. v. West Publishing Co.](#): contributory infringement is "personal conduct that encourages or assists [direct] infringement."

The court ultimately held that myVidster was not liable for contributory

infringement for two reasons. First, myVidster does not make any copies of Flava's videos—whether on its own initiative or at its users' direction—but instead links to videos on servers controlled by third parties. In bookmarking offending videos, myVidster's users were not copying such videos. And by embedding those videos on its site, myVidster was not furthering any copying. Rather, the court found that myVidster effectively acts as an exchange, connecting the server hosting the video and myVidster's users. Posner wrote: "[The user's] bypassing Flava's [pay wall](#) by viewing the uploaded copy is equivalent to stealing a copyrighted book from a bookstore and reading it. That is a bad thing to do (in either case) but it is not copyright infringement. The infringer is the customer of Flava who copied Flava's copyrighted video by uploading it to the Internet."

Second, the court found that myVidster had done nothing to encourage uploaders to upload Flava's videos. Therefore, myVidster did not "encourag[e]" infringement and was not a contributory infringer. As a result, myVidster had no need to resort to the § 512(c) safe harbors.

One of the most interesting aspects of the *Flava Works* opinion is its discussion of the various flavors (flavas?) of contributory infringement. Google and Facebook submitted an [amicus curiae brief](#) in which they argued that the connections between myVidster's (and other social bookmarking sites') activities and any copyright infringement by users are simply too attenuated to constitute either direct or contributory infringement. They argued that myVidster was, at most, "contributing to contributory infringement." Thus, myVidster's potential infringement was not "secondary," but rather, tertiary: the direct infringers are those who uploaded Flava's copyrighted material, those who bookmarked the videos are arguably "secondary" infringers, while myVidster might be a "tertiary" infringer. Posner [dismissed this argument](#), finding that common law notions of remoteness were

sufficient to deal with this “contributing to contributory infringement” situation: “An injury will sometimes have a cascading effect that no potential injurer could calculate in deciding how carefully to act. The effect is clear in hindsight—but only in hindsight.” For Judge Posner, even in social media situations, there’s no need for the direct-secondary-tertiary “layer cake” model; there is simply infringement, contributory infringement, and non-infringement. And regardless of the theoretical “level” of removal of myVidster from the underlying direct infringement, myVidster was not “materially contributing” to that infringing activity—that is, myVidster’s actions were too remote from the uploader’s infringement—and therefore it was not liable for contributory infringement by copying.

Judge Posner also addressed whether myVidster might be liable for contributory infringement based on public performance of Flava’s videos. The [Copyright Act](#) makes it unlawful “to transmit or otherwise communicate a performance . . . of the work . . . to the public . . . whether the members of the public capable of receiving the performance . . . receive it in the same place or in separate places and at the same time or at different times.” Posner identified two ways in which myVidster might infringe Flava’s performance right: “performance by uploading” and “performance by receiving.” On the “uploading” interpretation, “uploading plus bookmarking a video is a public performance because it enables a visitor to the website to receive (watch) the performance at will[.]” On the “receiving” interpretation, the performance occurs (or is, in other words, finalized) when the user clicks on and plays the video.

Posner dismissed the “uploading” view, arguing that myVidster is simply “giving web surfers addresses where they can find entertainment[.]” much like [TimeOut](#) and the [New Yorker](#) list the details of various social events happening in the real world. According to Posner, the only infringer on the “uploading” view is

the uploader himself. myVidster does not interfere with the data streaming directly from the host to the viewer, so myVidster did not contribute to the uploader’s infringement of Flava’s public performance right.

On the “receiving view,” the infringing act occurs when the myVidster users click “play” on Flava’s videos. Flava argued that, by providing an exchange that makes Flava’s videos available to myVidster’s users, myVidster provides “support services” without which “it would [have been] difficult for the infringing activity to take place in the massive quantities alleged.” Posner, however, was not persuaded by the “receiving” argument either. First, myVidster was not selling the allegedly infringing videos and thus had no direct pecuniary motive for pushing visitors to view Flava content bookmarked by the site’s users. Second, there was no substantial evidence that the videos were being accessed via myVidster rather than other websites. Thus, in Posner’s view, there was no basis to hold that myVidster was “abet[ting] others’ infringements” of Flava’s public performance right.

Judge Posner left open the possibility that myVidster had invited users to post infringing material, in which case it could be liable for [inducing infringement](#). Similarly, he stated that myVidster’s now-discontinued [sideloading](#) service constituted direct—not secondary—infringement. Sideloading typically involves the transfer of data between two local devices. myVidster’s service allowed premium members to back up bookmarked videos on myVidster’s servers. As at least one [commentator](#) has noted, this raises interesting issues for sites like [Pinterest](#) and other social networks that periodically sideload copyrighted material posted by users on the presumption that such sideloading is authorized by, and therefore done at the direction of, the user. If such actions constitute direct infringement, then the § 512(c) safe harbors may not be available.

Born to Mock: Trademark Holder’s Fight to Remove Mark on Kitsch Merchandise May Have Broad Legal Implications

Popular online marketplace [CafePress.com](#) suffered a legal setback in September 2012, when a U.S. District Court in the Southern District of New York denied CafePress’s motion for summary judgment against [claims of trademark infringement](#) in a case with potentially broad implications for social media sites that host user-generated content.

Social media and other sites that host user-generated content should remember that the DMCA safe harbors do not apply to claims of trademark infringement.

CafePress operates an online “print on demand” service that allows users to upload designs that CafePress then prints on a variety of items. The users receive a share of the money that CafePress makes when it sells items displaying the users’ designs. These items include everything from coffee mugs and [beer steins](#) to iPhone cases and [flip-flops](#). In 2009, guitar neck manufacturer Born to Rock

Design Incorporated (BTR), which owns a federal registration for the trademark “Born to Rock,” sent a letter to CafePress asking the site to stop selling merchandise displaying the mark. Since 2003, CafePress had produced a number of different items displaying the “Born to Rock” phrase, all based on designs provided by users—designs such as the following:



After CafePress refused to remove user designs incorporating the phrase, BTR filed a complaint for, among other things, trademark infringement. Following discovery, CafePress filed a motion for summary judgment, arguing that the “Born to Rock” designs were not used in commerce (an element of trademark infringement) and that, even if they were, CafePress’s use constituted “fair use”—i.e., a descriptive or ornamental use of the phrase “Born to Rock” in a non-trademark sense. The court struck down CafePress’s first argument outright, stating that CafePress was being “facetious” in arguing that it did not use the mark in commerce given that CafePress actually imprints the designs on merchandise and ships that merchandise to customers. In considering the fair use argument, the court acknowledged that certain uses of the “Born to Rock” designs may constitute non-trademark fair use (e.g., “Born to Ride / Born to Rock”), but concluded that CafePress could not rely on fair use as a blanket defense for *all* of the designs at issue.

Legal scholar Eric Goldman has pointed out that CafePress can raise other, stronger arguments in the future, including that the trademark is invalid and that consumers were not likely to be confused by CafePress’s use of the mark. Nonetheless, the district court’s denial of summary judgment does send a message to trademark holders: you can sue online service providers for trademark infringement based on user-generated content... and you just might win. Although the Digital Millennium Copyright Act (DMCA) creates a limited safe harbor for online service providers who promptly remove *copyright*-infringing user-generated content after receiving appropriate takedown notices, there is no equivalent safe harbor for content that infringes trademarks. (Interestingly, Chillingeffects.org, a website devoted to the DMCA and, specifically, to posting copies of third-party DMCA takedown notices, does suggest that “in the absence of any caselaw on the subject, should a trademark holder bring a claim

for contributory infringement, an [online service provider] might be able to mount a valid defense by analogy to [DMCA] section 512(c).”)

Social media sites in particular could be easy targets for trademark claims based on user-generated content, given that such sites often host “community pages,” placeholder web pages that end up serving as fan pages for brands without any authorization from the companies at issue. For example, compare this official Facebook page established by a trademark holder, with this community page run by a fan. In the wake of the above complaint against CafePress, social media sites and other websites that host user-generated content should remain aware of these trademark-related risks, and of the fact that the DMCA safe harbors do not apply to claims of trademark infringement.

The FTC’s Spokeo Settlement Highlights Social Media-Related Legal Risks

The Federal Trade Commission (FTC) recently reached an \$800,000 settlement with the data broker Spokeo, Inc. (“Spokeo”). The FTC’s complaint alleged violations not normally seen together: First, that Spokeo distributed personal information for background checks by employers in ways that failed to comply with the Fair Credit Reporting Act (FCRA) and, second, that Spokeo’s employees posted Spokeo product endorsements without revealing their connection to the company, in violation of Section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.”

The Alleged FCRA Violations

The FCRA imposes certain obligations on “consumer reporting agencies,” which

are generally defined as businesses that assemble or evaluate certain information about a consumer and furnish it to third parties for their use in determining the consumer's eligibility for credit, insurance, or employment. The FCRA requires a consumer reporting agency to follow specified procedures to help protect consumers' rights, including steps to ensure that each report it sells is used for a purpose specifically permitted by the law and that the information contained in the report is accurate. The law also requires a consumer reporting agency to inform each recipient of a consumer report of its obligations under the Act, including that it notify a consumer in the event that it takes adverse action against him or her based on information in the report (such as a decision to deny him or her credit or not to hire him or her).

Companies that compile or evaluate and then distribute consumer data should determine whether they need to comply with the requirements of the Fair Credit Reporting Act (FCRA).

Spokeo collects personal information about consumers from hundreds of online and offline sources—including social networks and marketing databases—and combines this information to create profiles on those consumers. Spokeo then sells access to these profiles. The FTC alleged that, because Spokeo marketed the profiles to human resources departments and others for use in the hiring process, it was a consumer reporting agency subject to the FCRA. According to the FTC, Spokeo did not, however, comply with the Act's

requirements. Moreover, even though Spokeo had changed its website terms of service to state that it was not a consumer reporting agency and to prohibit clients from using its information for purposes protected by the FCRA, Spokeo did not actually enforce those terms, such as by revoking the access of companies that it knew—or should have known—were using its consumer reports for employment purposes.

Although this is the FTC's first FCRA case involving the sale of data collected for employment purposes from social media and other online sources, it should not have come as a complete surprise, as this was not the first time that the agency had weighed in on the subject. In May 2011, FTC staff wrote to a company described as "an Internet and social media background screening service used by employers in pre-employment background screening," reminding it of the FCRA's applicability.

Even in light of these FTC activities, however, businesses may not appreciate just how broad the law's definition of a "consumer reporting agency" is. Companies that compile or evaluate and then distribute consumer data should seek to determine whether they need to comply with the FCRA's requirements. Further, companies that receive consumer reports from consumer reporting agencies—whether to make employment decisions or otherwise—are also bound by certain obligations under the FCRA and, potentially, state laws.

The Allegedly Deceptive Endorsements

Just a few years ago, the FTC updated its Endorsement Guides ("Guides") to address issues specific to social media marketing. Although the Guides do not have the force of law, they provide marketers with guidance from the FTC on avoiding potentially deceptive practices under Section 5 of the FTC Act. Even prior to this update, however, the Guides made clear that any connection between an endorser and the seller of the advertised product—such as

an employment relationship—must be disclosed, because such a connection affects the weight that consumers give to the endorsement. The message to companies: Create and enforce a social media policy that requires your employees to disclose the fact of their employment when talking about your products or services.

Spokeo allegedly did just the opposite: The FTC asserted in its complaint that Spokeo directed its employees to pose as ordinary consumers and post endorsements praising the company's products. What's more, Spokeo managers actually reviewed the endorsements and supplied the accounts that were used to make them—all to give the public the misleading impression that Spokeo had numerous happy customers. In the FTC's view, this practice was deceptive because, had consumers known that the endorsements were posted by the seller's own employees, they would have known that they should probably take the endorsements with a grain of salt. In its settlement with the FTC, Spokeo agreed not only to comply with the Guides going forward but to also remove all of the fake endorsements already posted.

A myth has developed among many companies seeking to exploit social media that the old rules do not apply in this new age. The *Spokeo* settlement is a stark reminder that the old rules do in fact apply, and that companies ignore those rules at their peril.

Update: What's Not to Like?

As we reported earlier in 2012, the Federal District Court for the Eastern District of Virginia held in *Bland v. Roberts* that merely "liking" a Facebook page is insufficient speech to merit constitutional protection.

In the case, former employees of the Hampton Sheriff's Office brought a lawsuit against Sheriff B.J. Roberts, in his individual and official capacities, alleging

that he violated their First Amendment rights to freedom of speech when he fired them, allegedly for having supported opposing candidate Jim Adams in the local election for Sheriff. Two of the plaintiffs had done nothing more than “like” Adams’s Facebook page.

Shortly after the district court ruled in favor of the defendants, the plaintiffs filed a [notice of appeal](#). Now [Facebook](#) and the [American Civil Liberties Union \(ACLU\)](#) have filed amicus briefs on behalf of the plaintiffs, arguing that “liking” something on Facebook is speech—or at the very least, expression—under the First Amendment, and thus should be entitled to constitutional protection.

In its amicus brief, [Facebook argues](#) that when the plaintiffs clicked the “like” button on Jim Adams’s campaign page, it was “the 21st-century equivalent of a front-yard campaign sign.” Facebook also notes, [as noted in our Socially Aware blog video interview with LexBlog](#), that clicking “like” is more than a passive

signal of approval because it has real effects on Facebook’s algorithm, including “notices and statements on a Facebook user’s profile page, in his or her friends’ news feeds, and in other places around the site.”

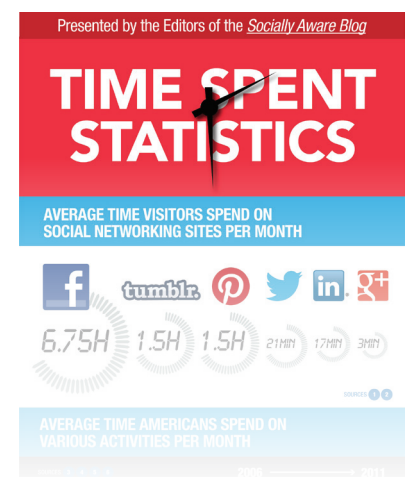
The [ACLU amicus brief](#) takes issue with the district court’s ruling that “liking” is not entitled to protection because it involves no actual statements. In response, the ACLU argues that even if “liking” something is not “pure speech,” courts have long recognized that First Amendment protection is not limited to actual words. The brief goes on to cite almost a dozen cases where conduct or expression has been held to be protected under the First Amendment. Further, the ACLU argues, whether someone presses a “like” button to express his thoughts or presses the buttons on a keyboard to write out those words, “the end result is the same: one is telling the world about one’s personal beliefs, interests, and opinions. That is exactly what the First Amendment protects, however that information is conveyed.”

The question of whether “liking” a Facebook page is or is not sufficient speech to merit constitutional protection demonstrates the challenge of interpreting traditional legal regimes in the Internet context.

This case is a prime example of the courts’ challenge of interpreting traditional legal regimes in dynamic, Internet contexts—one that we will continue to follow as it progresses.

Infographic: The Growing Impact of Social Media

How much time do people spend each month visiting social networks? Where do more people go to watch online video than anywhere else? How do Americans watch TV these days, and how much of it do they watch online? And just how ubiquitous *has* social media become? All this, and much more, can be found in the latest infographic from the editors of [Socially Aware](#)—click [here](#) or visit www.SociallyAwareBlog.com/TimeSpentStats to view the full infographic!



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 nine 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.

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.