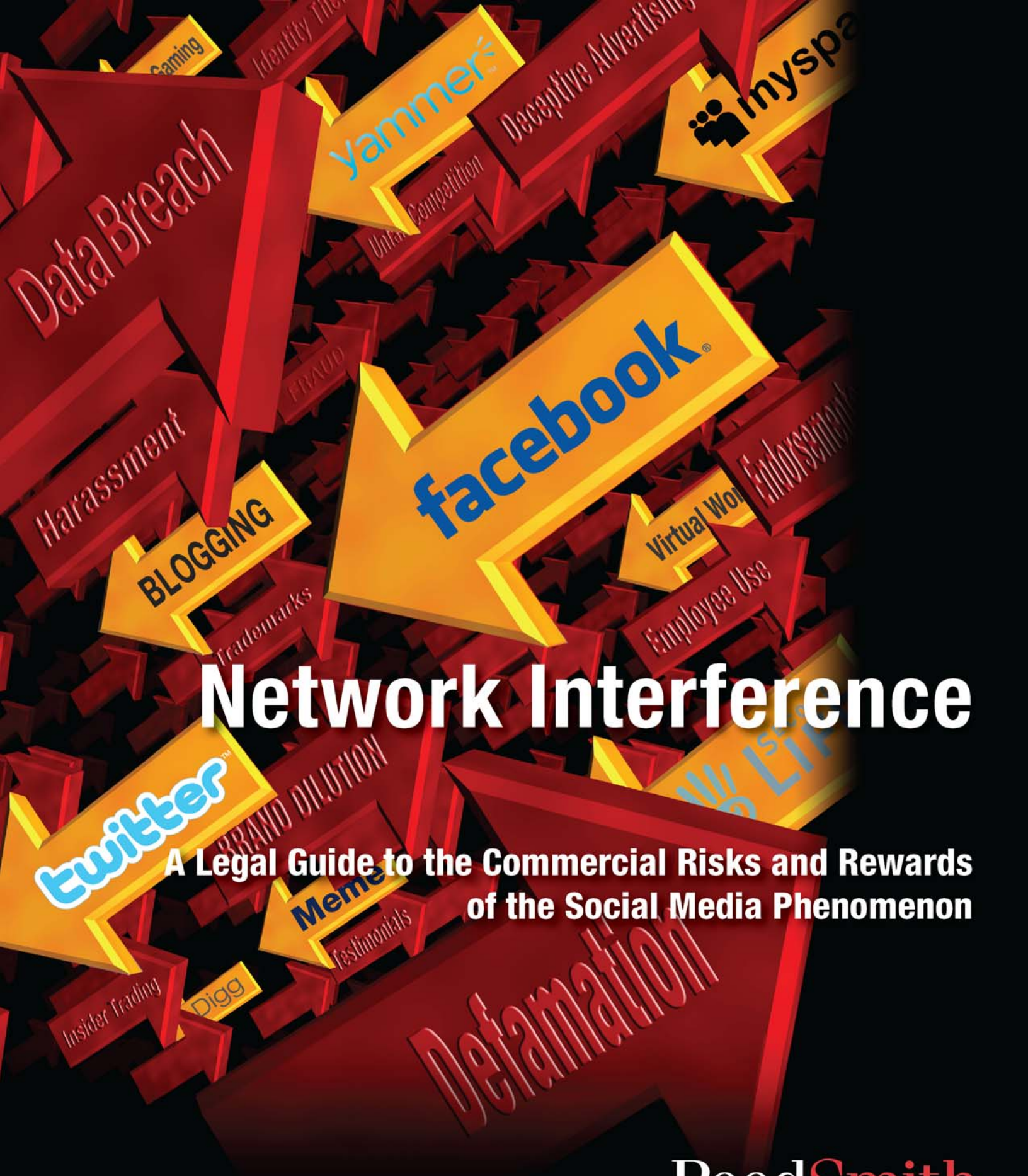


Network Interference

A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon

ReedSmith

reedsmith.com

— PREFACE —

In Summer 2009, I watched in wonder as Twitter became a vital communications link in the election riots in Iran. Until then, I didn't think much about social media and hadn't done much with my Facebook or LinkedIn accounts. They just didn't seem that relevant to me. Then the marketplace exploded. Government agencies started opening Facebook and Twitter accounts. Major companies signed on as well and began using social media platforms as communication centers for employees and customers. There was an avalanche of new social media sites, each with its own twist. And people were making money from the sites. A lot of money.

It occurred to me that the legal issues were far deeper than first met the eye. Yet companies and employees were populating sites in droves, oblivious to those risks. I further learned, upon talking to my partners, that we were advising companies across practices on issues central to this new media. Collectively, we agreed to team up to present companies with a holistic solution—Reed Smith's Social Media Task Force. From these conversations, the idea of this White Paper was born.

Partners and associates from many of our practice groups have provided chapters to help our clients navigate through this rapidly changing landscape. Stacy Marcus and Rita DeCaria took up the laboring oars of organizing and editing. I had the easy job—wrangling writers and reviewing the final copy.

This was truly a team effort, and special thanks also go to the following people: Eric Alexander, Jesse Ash, Chris Bennett, Paul Bond, Maureen Cain, Darren Cohen, Gerry DiFiore, Michael Golebiewski, Amy Greer, Daniel Herbst, Mark Hersh, Greg Hessinger, John Hines, Andrew Hurst, Tony Klapper, Janice Kubow, Leah March, Andrew Moss, Amy Mushahwar, Meredith Pikser, Joe Rosenbaum, Carolyn Rosenberg, Casey Ryan, Nancy Schulein, Amber Spataro, Sandy Thomas, Lois Thomson, Jacob Thride, and Anthony Traymore.

Most importantly, this White Paper will forever be a living document as we add more chapters and update those we have, making sure it remains the definitive source for legal issues in social media.

We welcome your ideas and comments as well. If you have anything you'd like to share with us—good or bad—please send it to socialmedia@reedsmith.com.

Thank you.

Douglas J. Wood
Editor

— EDITORS —

Douglas J. Wood – dwood@reedsmith.com

Stacy K. Marcus – smarcus@reedsmith.com

Joseph I. Rosenbaum – jrosenbaum@reedsmith.com

— TABLE OF CONTENTS —

Welcome to the New World

Social media is a revolution in the way in which corporations communicate with consumers. This White Paper will help you to maximize the huge potential benefits of this revolution and protect against the inherent legal risks surrounding this phenomenon. In this document, you will find practical, action-oriented guidelines as to the state of law in the following areas: Advertising & Marketing; Commercial Litigation; Data Privacy & Security; Employment Practices; Government Contracts & Investigations; Insurance Recovery; Litigation, Evidence & Privilege; Product Liability; Securities; and Trademarks

What is Social Media and What Changes is it Affecting?

Everyone has heard of Facebook, YouTube, and MySpace. These are just the tip of the iceberg. There are hundreds of social media sites with tens of millions of participants. And it's not just individuals. Multinational companies and their CEOs are increasingly active in the social media space via blogs, Facebook fan pages, and YouTube channels. Everyone is a user and, as with every new communication channel—billboards, radio, television, the Internet—there is huge potential—and huge potential risks.

The speed of development in social media outstrips corporate risk management capability. It took radio 38 years to reach 50 million listeners. Terrestrial TV took 13 years to reach 50 million users. The Internet took four years to reach 50 million people. In less than nine months, Facebook added 100 million users[1].

It's All About the Conversation

One-way communications with advertising, press releases, labels, annual reports, and traditional print media is going the way of the dinosaur. We no longer just listen. We now engage in a conversation. What was said in the living room is now published on Facebook. What we do in public and private is now broadcast on YouTube. What employees talked about at the water cooler now appears as tweets on Twitter. All of it memorialized in discoverable form. All of it available to millions with the simple press of "post."

Social media is about "changing the conversation"—getting people to say the right things about your company and its products and services.[2]

Managing Reputation – The Asymmetrical Consumer Relationship

Historically, brand owners were able to determine the relationship that consumers had with their brand. Now, thanks to social media, consumers are the ones who increasingly define how the brand is perceived.

A major retailer asked a simple question on its Facebook page—"What do you think about offering our site in Spanish?" According to its Senior Director, Interactive Marketing and Emerging Media, the response "…was a landmine. There were hundreds of negative responses flowing in, people posting racist and rude comments. Our contact center was monitoring this, and they were crying, waiting for a positive comment to come in." The racist and negative responses posted by purported "fans" were so bad that the site was shut down with a spokesperson noting, "We have to learn how to respond when negative comments are coming in."[3]

United Airlines broke a passenger's guitar. They handled his complaint through traditional procedures, eventually refusing to pay for $1,200 in repairs. In response, the passenger launched a humorous music video to draw attention to United's consumer support incompetence on YouTube. [4] To date, there have been nearly 6 million views of the video. After two other videos, and United donating the cost of the guitar repairs to charity per the musician's requests, United managed to lose the musician's bags, an event that was reported to millions in the blogosphere.[5] The story was a lead story on CNN's Situation Room, reported by anchor Wolf Blitzer.[6] As a result, United's stock value fell considerably.[7] To add insult to injury, the incident is impacting the law. U.S. Sen. Barbara Boxer (D-Cal.) is championing the Airline Passenger Bill of Rights Act of 2009[8], citing the United debacle.[9] We can't help but wonder if United would have fared better if it had discarded the old way and instead engaged in the conversation using the same social media platforms that were used to attack their brand.

For at least one major company, engaging made all the difference. Two employees of Domino's Pizza posted a disgusting video on YouTube in which they adulterated the chain's food. In addition to reporting the video to the police, Domino's Pizza's CEO posted his own video, apologizing for what consumers saw and assuring them that such things were not condoned nor practiced at Domino's. It all made the "Today Show" and other media reports.[10] Both traditional media and the blogosphere applauded his open communication and willingness to engage in a conversation about the problem.[11] Rather than seeing its brand value and reputation take a major blow, it survived the negative media.

As social media pioneer Erik Qualman puts it, "A lot of companies say we're not going to do social because we're concerned about letting go of the conversation, and what I argue is that's like an ostrich putting their head in the sand. You're not as powerful as you think. You're not going to enable social to happen, it's happening without you so you might as well be part of the conversation."[12]

The New World

The key lesson is that rather than trying to control, companies must adopt an altered set of rules of engagement.

What You Need to Do

Every lawyer needs to take some important steps if he or she is going to be prepared for the new media revolution. Here are a few:

- Read this White Paper
- Surf the social media sites and read their terms and conditions
- Join Facebook and LinkedIn and perhaps other social media sites
- Review each site's terms and conditions
- Audit your company's social media programs. Find out what your company and your employees are doing. Do they have any customized pages on platforms like Twitter and Facebook? If so, make sure they're complying with the site's terms and conditions, as well as your corporate communications policies. Are they blogging? Are employees using social media during work hours?
- Find out what your competitors and your customers are doing
- Consider adopting a social media policy for both internal and external communications. But be careful to keep on strategy, don't ban what you stop, and keep in mind the basic rules of *engage, participate, influence, and monitor*.
- Bookmark websites and blogs that track legal developments in social media, including, *Adlaw by Request* (www.adlawbyrequest.com) and *Legal Bytes* (www.legalbytes.com)

It is not going to be business as usual. Social media has forever changed the brand/customer relationship. It challenges brand owners fundamentally to reappraise the way they market themselves. This White Paper will be an invaluable tool in helping you to do just that. Welcome to the New World

— CHAPTER 1 —

Advertising & Marketing

Chapter Authors

Gregory J. Hessinger, Partner – ghessinger@reedsmith.com

Stacy K. Marcus, Associate – smarcus@reedsmith.com

Anthony S. Traymore, Associate – atraymore@reedsmith.com

Introduction

This chapter looks at the relationship between social media and advertising and marketing practices.

As an emerging technology with nearly limitless boundaries and possibilities, social media gives consumers unprecedented engagement with a brand. Consumers are empowered. They aren't just buying a product or service online, they are discussing, reviewing, endorsing, lampooning, comparing and parodying companies and their brands. They aren't simply being targeted for advertising, in many cases they are participants in the creation and distribution of advertising. Companies can better enable, influence, monitor, react to and, hopefully, monetize the consumer conversations taking place in social media, and can better engage and interact with the consumer directly with their brands—but it's critical to understand and navigate the legal minefields that are both dynamic and evolving as the media evolves.

Why are advertisers and marketing professionals drawn to social media? Because more than 1.6 billion people use the Internet every day[13], and, according to Nielsen, consumer activity on social networking and blogging sites accounted for 17 percent of all time on the Internet in August 2009, up from 6 percent a year ago.[14] The Internet audience is larger than any media audience in history, and it is growing every day. It's those eyeballs that marketers want.

Nielsen estimates that ad spending on social networking and blogging sites grew 119 percent, from an estimated $49 million in August 2008 to $108 million in August 2009.[15] Expressed as a percentage of total U.S. online ad spend, ad expenditures on social networking sites climbed from 7 percent in August 2008 to 15 percent last month.[16] Where are companies spending these dollars? The possibilities are numerous.

We begin by examining the use of social media to increase brand awareness. Branded channels, gadgets, widgets, promotions such as sweepstakes and contests within and even across social media platforms are a few of the ways companies are using social media to increase brand awareness. Even companies that are not actively using social media platforms to engage consumers must monitor social media outlets for comments made about the company or its brands. Social media cannot be ignored and this section explores the legal implications of marketing in this manner?

Next, we look at the use of social media to foster brand engagement and interaction. Many companies are moving beyond simply having a page on Facebook, MySpace or YouTube, and are encouraging consumers to interact with their brand. Companies are using social media to provide customer service and get product reviews. Marketers seek to engage the consumer in developing user-generated content ("UGC") around their brands for advertising and actively solicit their social networks to create buzz, viral and word of mouth advertising campaigns. Who controls and retains liability for the statements made and content provided in the social media universe? Who owns the content? Will brand owners lose control of their brands?

Finally, we explore the impact of social media on talent rights and compensation. As discussed above, increasingly, ad spend is moving online. Along with this shift, the line between "content" and "advertising" has become blurred. Celluloid is being replaced by digital files and projectors by flat screens and monitors. What once aired only on television is now being moved over to the

Internet by content owners and advertisers, or is going viral thanks almost entirely to consumers with a little encouragement from advertisers. We will examine how this shift impacts talent compensation and discuss its application to the Screen Actors Guild ("SAG") and American Federation of Television and Radio Artists ("AFTRA") commercials contracts.

Social Media in Action in Advertising and Marketing

Brand Awareness

The official Starbucks page has more than 4.7 million fans and counting. The Starbucks YouTube channel has nearly 3,800 subscribers and 68 videos. On Flickr, the Starbucks group has 4,571 members and nearly 14,800 photos. And more than 460,000 people are following Starbucks on Twitter. Starbucks' own social network, Starbucks V2V, has more than 21,000 members.

Branded Pages

Branded social media pages created and hosted using a third-party service allow companies to quickly and easily establish a social media presence. In order to do so, companies, like individuals, must register and agree to abide by the terms of use and policies that apply to these services and host companies. As discussed in "Promotions and Contests," below, this may not only restrict a company's ability to use the branded page for promotional and advertising purposes, but also grant or restrict rights within the media with which a brand owner might not otherwise have to contend. The third party bears much of the responsibility for regulating the actions of the users who access, use and interact with the service. The third party, for example, is responsible for responding to 'take down' notices received pursuant to the Digital Millennium Copyright Act ("DMCA") and for establishing age limits for users (*See also Chapter 2 Commercial Litigation*). The terms of service applicable to Facebook and YouTube specifically prohibit use by children under the age of 13, while Twitter allows access only by individuals who can enter into a binding contract with Twitter.[17] Facebook, YouTube and Twitter prohibit the uploading or posting of content that infringes a third party's rights, including intellectual property, privacy and publicity rights, and provide instructions for submitting a DMCA take-down notice.[18] Although the third party's terms of service provide a framework for both a company's and individual user's activities, can a company afford not monitor its branded page for offensive or inappropriate content, trademark or copyright infringement, or submissions obviously made by or containing images of children?

Creating a presence and beginning the conversation is easy. Controlling the conversation is nearly impossible. Looking again at Starbuck's as an example, a search for "Starbucks" on Flickr currently yields more than 261,000 results, on MySpace yields 500 results, and more than 500 unofficial "Starbucks" pages on Facebook. This is the current state of affairs, despite the fact that as a part of the registration process for a page, Facebook asks that individuals "Please certify that you are an official representative of this brand, organization, or person and that you are permitted to create a Facebook Page for that subject," coupled with an electronic signature. As an additional deterrent, Facebook includes the following note: "Fake Pages and unofficial 'fan pages' are a violation of our Pages Guidelines. If you create an unauthorized Page or violate our Pages Guidelines in any way, your Facebook account may be disabled." Similarly, Twitter has an "Impersonation Policy" that prohibits "non-parody impersonation."[19]

Despite these efforts by social media platforms such as Facebook and Twitter, can these 'legal' conditions and requirements realistically act as a deterrent or a meaningful enforcement mechanism? More significantly, will a company be forced to rely upon these third party's to provide remedies or enforce these terms before acting—or instead of acting? So what are a company's options in managing its brand image? While a company could have a claim for copyright or trademark infringement (*see Chapter 10, Trademarks*) and could attempt to shut down impersonator and unofficial sites by contacting the social media platform to demand that the infringer and infringing material be removed, these measures could become (and may already be) virtually impossible to implement due to sheer volume. Further, depending upon the message being conveyed on an unofficial page, a company might not want to shut it down. For example, there are three unofficial "I love Starbucks" pages and more than 500 "I love Starbucks" groups. If a consumer cares for a Frappaccino, they can join one of the more than a dozen groups dedicated to various flavors. But for every "I love Starbucks" page or group, there is an "I hate Starbucks" group (more than 500) or "Starbucks sucks" page (211). How does a company respond to these so-called "suck sites"? As previously mentioned, a company could try to litigate on the basis of intellectual property infringement, but that could prove to be an endless battle.

Promotions and Contests

Many companies are using their social media presence as a platform for promotions, offering sweepstakes and contests within or founded upon social media and user networks. There are giveaways for the first ten people to re-Tweet a Tweet. Companies can partner with YouTube to sponsor contests that are featured on YouTube's Contest Channel or sponsor contests available on a company-branded channel. While YouTube's terms of service are generally silent on the issue of sweepstakes and promotions, Facebook's terms of service specifically prohibit the offering of contests, giveaways or sweepstakes on Facebook without their prior written consent. Facebook's terms also specifically require that the sponsor take full responsibility for the promotion and follow Facebook's Promotion Guidelines as well as applicable laws. Facebook's Promotion Guidelines prohibit: (1) the use of Facebook's name, trademarks, trade names, copyrights, or any other Facebook intellectual property in the rules to or any other materials relating to the promotion; (2) directly or indirectly indicating that Facebook is a sponsor or administrator of the promotion; or (3) administer the promotion on the Facebook site, other than through an application on the Facebook Platform. Many companies, however, appear to be ignoring Facebook's terms.

Other companies have taken their contests off of a particular social media platform and instead operate a contest-specific URL. One such company is Qwest. Qwest recently launched a social media contest to raise awareness about the importance of backing up important data. The contest, located at a dedicated URL and modeled after Qwest's existing "Crash Happens" advertising campaign, encourages people to submit their stories of data loss and recovery to help others learn from their experiences (*See "User-Generated Content," below for issues relating to UGC*). Entrants have a chance to win a prize package worth more than $1,000. In a unique twist, in addition to the Grand Prize and Runner-Up prize, a prize will be awarded for the "Most Viral" submission. The Most Viral winner is the participant who creates the entry that gets the most attention across the Internet on sites other than Brickfish (the host of the contest). If a participant uses the "Post to Websites" or "Embed" tools to spread his or her entry across the Internet, he or she becomes eligible for the Most Viral prize. It doesn't take much imagination to come up with the legal issues and challenges—consumer and regulatory—that might be raised. How are eligible entrants determined? How can one be sure who is "most viral" when control (and even metrics), may be outside the control of the sponsor and the platform? And what about scams, hackers, spoofers and others who might exploit the promotion illicitly to their own gain? Qwest is promoting the "Crash Happens" contest through typical online marketing channels, as well as a Twitter campaign that offers tweeters a chance to win free Qwest High-Speed Internet service for a month for re- Tweeting updates regarding the "Crash Happens" contest.

Regardless of the platform or website a contest is featured on, the same laws apply online as in offline contests, but they may apply in unique or novel ways and their applicability may be subject to challenge. Because social media is often borderless and global, companies must also consider the possibility that individuals from across the globe may find out about the contest and wish to enter. Unless a company plans to research the promotion and sweepstakes laws in every country around the globe (and translate the official rules into every language), eligibility should be limited to those countries where the company does business and/or has legal counsel. This represents both an opportunity and a challenge—both fraught with legal and regulatory possibilities.

In the United States[20], a sponsor cannot require entrants to pay consideration in order to enter a sweepstakes. Unlike skill-based contests, the golden rule of "no purchase necessary to enter or to win" applies. In addition, depending upon how the promotion is conducted and what the aggregate value of prizes awarded in the promotion are, New York, Florida and Rhode Island have registration requirements (New York and Florida also require bonding[21]). In New York and Florida, where the aggregate prize value exceeds $5,000, a sponsor must register the promotion with the state authorities and obtain and file with the state a bond for the total prize amount.[22] In Rhode Island, where the aggregate prize value exceeds $500 and the promotion involves a retail sales establishment, a sponsor must register the promotion with the Rhode Island Secretary of State.[23]

Brand Interaction

Bloggers

"People are either going to talk with you or about you."[24] So how do you influence the conversation? Many companies are turning to amplified word-of-mouth marketing, by actively engaging in activities designed to accelerate the conversations consumers are having with brands, including the creation of Facebook applications based on a company or its product. (*See Chapter 2 Commercial Litigation*,) In July 2009, for example, Starbucks created a Facebook application where users could share a virtual pint of ice cream with friends. Other

examples include the use of third-party bloggers to create product reviews, offering giveaways on third-party blogs or creating a company-sponsored blog (*see "Customer Service and Customer Feedback," below*).

Companies often provide products to bloggers so that the blogger can write a (hopefully favorable) review of the product. While this practice is generally acceptable, companies and bloggers who fail to disclose the connection between blogger and company face regulatory scrutiny and consumer backlash. In Spring 2009, Royal Caribbean was criticized for posting positive reviews on travel review sites with a viral marketing team, the "Royal Champions," which was comprised of fans who posted positive comments on various sites such as Cruise Critic. In return for positive postings, the Royal Champions were rewarded with free cruises and other perks. Royal Caribbean has acknowledged that the Royal Champions program exists, but denies that it was ever meant to be secretive or that members were instructed to write positive reviews.

In addition to backlash from consumers who might feel as if they've been duped or that a blog is a glorified advertisement and the blogger an instrument of a particular company, companies and bloggers who fail to disclose material connections (such as the provision of free products or other perks to the blogger) may come under regulatory scrutiny. The Federal Trade Commission ("FTC") recently revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising (the "FTC Guides')[25]. The FTC Guides provide a general principle of liability for communications made through endorsements and testimonials: "Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failing to disclose material connections between themselves and their endorsers. Endorsers also may be liable for statements made in the course of their endorsements."[26]

In general, a company that provides products to a blogger for purposes of a product review should never instruct the blogger regarding what to say in the review, or ask to review or edit the review prior to posting. While companies should provide bloggers with up-to-date company-approved product information sheets, those information sheets should not reflect the company's opinion or include prices. In the event of a negative review, the company has the option of not providing products to the blogger for future reviews. The company should also caution its personnel about engaging in inflammatory disputes with bloggers ("flaming") on any blogs. In addition, since under the FTC Guides a company could be liable for claims made by a blogger, the company should monitor product reviews made by bloggers to ensure that the claims made are truthful and can be substantiated.

Customer Service and Customer Feedback

Blogs also foster customer feedback and engagement with a brand. General Motors, for example, has at least two blogs: the Fast Lane[27] and the Lab[28]. According to General Motors, the Fast Lane is "a forum for GM executives to talk about GM's current and future products and services, although non-executives sometimes appear here to discuss the development and design of important products. On occasion, Fast Lane is utilized to discuss other important issues facing the company."[29] The Lab is "a pilot program for GM, an interactive design research community in the making."[30] The Lab lets consumers "get to know the designers, check out some of their projects, and help [the designers] get to know [the consumers]. Like a consumer feedback event without the one-way glass."[31] Both General Motors blogs, of course, link to General Motor's Facebook page where a consumer can become a fan. Similarly, Starbucks has its "Ideas In Action" blog where consumers share ideas with the company. The customer feedback received via the blog and social networks led to the creation of a store-finding and menu-information application for the iPhone, and a second application that will let customers use the iPhone as their Starbucks card. According to Stephen Gillett, Starbucks' chief information officer, "We think it's really talking to our customers in new ways."[32]

Once you've started the conversation, you can use social media to provide nearly instantaneous customer service and receive customer feedback. Major credit card companies and international banks are providing customer service via Twitter. Think kids say the darndest things? Wait until you see what customers say once they start talking.

A major retailer launched its Facebook page in July 2009. In September, the company posted a seemingly innocent question: "What do you think about offering [our site] in Spanish?" The company didn't get the constructive dialogue that it was looking for. According to the company's senior director of interactive marketing and emerging media, "It was a landmine. There were hundreds of negative responses flowing in, people posting racist, rude comments." Oops, now what? Do the tenets of free speech demand that a company leave such comments posted on its branded social media page? Or, can the company selectively remove such comments? In this case, they removed the post, hoping that the commenters would go away. They did…this time.

Still doubt the power of social media? In September 2009, a major washing machine company interacted with a so-called 'mommy-blogger' through Twitter, turning what started out as a negative into a positive. After what she described as a frustrating experience with the company's customer service representative and her new washing machine, Heather Armstrong, Tweeter and author of Dooce.com, aired her grievances with the company and its product on Twitter. Ms. Armstrong sent a Tweet to her more than 1 million followers urging them not to buy from the company. Three minutes later, another Tweet with more criticism. Another three, equally barbed Tweets followed. Within hours several appliance stores had contacted Ms. Armstrong via Twitter offering their services. Then came a Tweet from the manufacturer asking for her number, and the next morning a company spokesperson called to say they were sending over a new repairman. By the following day, the washing machine was working fine. That's an example of tackling a social media problem creatively rather than deciding to let it slide, and turning it into a positive customer experience. And another twist: @BoschAppliances offered Ms. Armstrong a free washing machine, which went to a local shelter.

So what does a company do if it finds itself or its products the subject of a negative or false post? First, it depends on where the post was made. Was it a company-operated blog or page or a third-party site? Second, it depends on who posted the negative comment. Was it a company employee? (*See Chapter 4 Employment*) Was it the author of the blog? Was it a third-party commenter on a blog? Was it a professional reviewer (journalist) or a consumer? Finally, the content of the post should be considered. Is a right of free speech involved? Was anything in the post false or defamatory (*See Chapter 2 Commercial Litigation*)? Companies should seek to correct any false or misleading information posted concerning the company or its products. This can be done by either seeking removal of the false post or by responding to the post to provide the public with accurate information. Where a post is defamatory, litigation may be an option. (*See Chapter 2 Commercial Litigation*). In the case of a negative (but truthful) product review or other negative opinion posted about the company, if the comments are made on a company-operated blog or page, the company, has the right to remove any posting it desires, subject, of course, to its policies and the terms on which the blog is made available. Where comments are made on a third-party's blog, a company could attempt to contact the author of the blog and seek removal of the post. However, depending upon the content of the post, it may not be in the company's best interest to take it down.

One of the central tenets of social media is open dialogue. Where a company avails itself of the benefits of social media but then inhibits the conversation by selectively removing posts, it may face a public-relations fiasco. One approach to responding to negative posts may be to have an authorized company representative respond to the post on behalf of the company in order to further engage the consumer in dialogue. If a company prefers not to have such a conversation in an open forum, the company could seek to contact the poster offline to discuss the poster's negative opinion of the company or its products. This is the approach that this company took when faced with negative Tweets from Ms. Armstrong.

User-Generated Content

UGC covers a broad spectrum of content from forum postings, to photos to audio-visual content such as, video and may provide the greatest potential for brand engagement. Companies frequently and increasingly create promotions around UGC, for example, urging consumers to submit content-rich descriptions of why they love a certain product or service. Don't think, however, "the consumer did it" is an iron-clad defense against claims of intellectual property infringement or false advertising. Especially in connection with contests that are set up as a comparison of one brand to another, things can get dicey. For example, Quiznos ran the "Quiznos v. Subways Ad Challenge," which solicited videos from users depicting that Quiznos' sandwiches have more meat than Subway's sandwiches. In 2007, Subway filed a lawsuit against Quiznos[33] claiming that by airing the winning video from the Quiznos contest, Quiznos had engaged in false and misleading advertising under the Lanham Act. As of the publication date of this chapter, the case was still in discovery, but Subway did survive a motion to dismiss filed by Quiznos.

As discussed in the section on "Branded Pages," above, if a company is accepting UGC submissions through use of a third-party platform (*e.g.*, Facebook or YouTube), odds are that the third party's terms of service already prohibit content that is infringing, defamatory, libelous, obscene, pornographic or otherwise offensive. Nonetheless, whenever possible, a company should establish community requirements for UGC submissions prohibiting, for example, infringing or offensive content. Similarly, although the third-party's terms of service most likely provide for notice and take-down provisions under the DMCA, companies should have procedures in place in the event they receive a notice of copyright infringement. Another reason to implement your own policy is that the services such as Facebook and Twitter may themselves have a

"safe harbor" defense as Internet service providers under the DMCA, whereas a company using an infringing work in a commercial context, whether or not through a third-party service, would not likely have such a defense available to it should an infringement claim arise. Although the third-party's terms of service provide a framework for both a company's and an individual user's activities, it is still recommended that a company monitor its branded page for offensive content, blatant copyright infringement, or submissions obviously made by, or containing, images of children. In advance of the UGC promotion, companies should establish policies concerning the amount of monitoring, if any, they plan to perform concerning content posted via their branded pages.

In addition to issues relating to content and intellectual property, companies should take steps to ensure that UGC displayed on their social media pages does not violate the rights of publicity of the individuals appearing in the displayed content. In January 2009, a Texas teenager and her mother sued Virgin Mobile for using one of her personal photos uploaded on Flickr for an Australian advertisement. The lawsuit insisted that Allison Chang's right-of-publicity had been exploited and that the use of her photo violated the open-source license under which her photo was submitted. Although the case was dismissed over a discrepancy in jurisdiction, the message is clear that if you seek to use UGC in a commercial context, whether or not on a social media page, best practice would be to obtain releases from any individuals depicted in your work.

Companies should make clear that by submitting UGC to the company, the submitter is granting the company a worldwide, royalty-free right and non-exclusive license to use, distribute, reproduce, modify, adapt, translate, publicly perform and publicly display the UGC. However, this does not give a company a license to transform the UGC into a commercial or print advertisement. In fact, in the event that a company seeks to transform a UGC video into a television commercial or made-for-Internet commercial, the company must obtain a release from any individuals to be featured in the ad and take into consideration the SAG and AFTRA requirements set forth in the commercials contract.

Talent Compensation

Commercial or Content?

In traditional television and radio media, the 30-second spot has reigned supreme as the primary advertising format for decades. Within that format, in order to help create compelling TV and radio spots, advertisers have frequently engaged professional on-camera and voiceover actors pursuant to the terms contained in industry-wide union contracts with the Screen Actors Guild ("SAG") and the American Federation of Television and Radio Artists ("AFTRA"), as well as musicians under a contract with the American Federation of Musicians ("AFM").[34] Those contracts dictate specific minimum compensation amounts for all performers who appear in commercials, depending upon the exhibition pattern of those spots.

Now, with companies rapidly shifting advertising dollars online, the cookie-cutter paradigms of traditional media have given way to the limitless possibilities of the Internet, mobile and wireless platforms and other new media—including social media. While 30-second spots remain one part of the new media landscape, creative teams have been unleashed to produce myriad forms of branded content that straddle traditional lines separating commercials and entertainment. This has understandably created confusion and uncertainty amongst, advertisers, agencies, talent and studios, to name only a few of the major players, with respect to the applicability of the SAG, AFTRA and AFM contracts in these unique online and wireless venues.

As a threshold matter, it is important to note that the SAG, AFTRA and AFM contracts apply only to Internet/New Media content that falls with the definition of a commercial. Commercials are defined as "short advertising messages intended for showing on the Internet (or New Media) which would be treated as commercials if broadcast on television and which are capable of being used on television in the same form as on the Internet." Put simply, if the content in question cannot be transported intact from the Internet to TV or radio for use as a commercial, then it is not covered by the union contracts and the advertiser is not obligated to compensate performers in accordance with those contracts, and can negotiate freely for appropriate terms. Thus, branded entertainment content and other forms of promotion that don't walk and talk like a commercial will not fall within the coverage of the union contracts.

Made Fors and Move Overs

If the content in question does fall within the definition of a commercial, the advertiser must determine whether the content constitutes an original commercial designed for Internet/ New Media exhibition (a so-called "Made For") or an existing TV or Radio commercial transported to the Internet/New Media (a "Move Over").

If the commercial is a Made For, under current provisions in the union contracts, advertisers may negotiate freely with the performers for appropriate terms, with no minimums required, except that pension and health contributions must

be paid on any amounts paid. Note, however, this period of "free bargaining" will expire April 1, 2011, at which time contractual minimums will apply absent any new understandings mutually agreed upon.

In the case of Move Overs, the union contracts do provide for minimum levels of compensation, depending upon the length of use for the spot. For eight weeks or less, performers must be paid 133 percent of the applicable session fee. For a one-year cycle, payment equals 350 percent of such fee.

User Placed or Generated Content

As noted above, the union contracts that govern the payment of performers are generally based upon the exhibition patterns for commercials. But what happens when we enter a world where advertisers no longer control where and when commercials appear (*e.g.*, YouTube)? Or to go even one step further, what happens when the advertiser doesn't even produce the commercials? Is the advertiser obligated to pay the actors under the union agreements? The answer is "no," but the person who posted the materials without permission is liable for invasion of privacy and publicity. Unfortunately, the pockets of those posters are generally too shallow to warrant an action by the actor.

These are fertile areas for disagreement between the advertising industry and the unions. But the industry position is clear: an advertiser cannot be held liable for compensating performers for an unauthorized exhibition of a commercial, nor is that advertiser responsible for policing such unauthorized use. Similarly, an advertiser cannot be held responsible for paying performers who appear in user-generated content, so long as the advertiser hasn't actively solicited and exhibited that content.

Current Legal and Regulatory Framework in Advertising

Depending on the advertising activity, various Federal and/or State laws may apply including, for example, Section 5 of the FTC Act (*See Chapter 2 Commercial Litigation)*, the Lanham Act (*See Chapter 2 Commercial Litigation and Chapter 10 Trademarks*), the DMCA, the CDA (*See Chapter 2 Commercial Litigation*), CAN-SPAM and state unfair trade practice acts.

Bottom Line—What You Need to Do

Social media implications and applications to advertising and marketing cannot be ignored. That is where the consumers are, and where consumers go, marketing dollars ultimately follow. All companies, regardless of whether or not they elect to actively participate in the social media arena, should have policies in place to determine how to respond to negative comments made about the company and/or its brands. Companies that seek to play a more active role should have policies in place that govern marketing agency and/or employee interaction with social media, as well as the screening of UGC. It is critical, however, that companies not simply adopt someone else's form. Each social media policy should be considered carefully and should address the goals and strategic initiatives of the company, as well as take into account industry and business specific considerations.

— CHAPTER 2 —

Commercial Litigation

Chapter Authors

John L. Hines, Jr., Partner – jhines@reedsmith.com

Janice D. Kubow, Associate – jkubow@reedsmith.com

Introduction

This chapter explores emerging exposures associated with false advertising and defamation in social media.

The ever-growing number of "conversations" in social media venues creates new opportunities for advertisers to promote their brand and corporate reputation. These same conversations, however, create new risks. Online disparagement of a corporation or its products and/or services through social media can spread virally and very quickly, making damage control difficult. Accordingly, corporations need to be aware of their rights and remedies should they fall prey to harmful speech on the Internet. An organization also needs to understand how to minimize its own exposure and liability as it leverages social media to enhance its brand and reputation.

Within the context of social media, the two greatest risks to brand and reputation are, respectively, false advertising and defamation. Within the realm of false advertising, companies need to pay attention to new risks associated with the growing phenomenon of word-of-mouth marketing.

Social Media in Action in Commercial Litigation

False Advertising and Word-of-Mouth Marketing: Understanding the Risks

The presence of social media increases the risk that your organization will be touched by false advertising claims– either as a plaintiff or a defendant. First, more communication means more opportunity for miscommunication generally and for a misstatement about your or your competitor's brand. Compounding this risk is the fact that social media marketing and sales channels (including word-of-mouth marketing programs) are now highly distributed, making enforcement of centralized communication standards difficult. Finally, social media frequently operates as a kind of "echo chamber": consumers hear their likes and dislikes repeated back to them, amplified, and reinforced by those who share similar feelings.[35] In light of all these factors, the growth of social media is likely to see false advertising claims skyrocket. Indeed, it is worth noting that a 2008 Federal Judicial Center Report concluded that between 2001 and 2007, the number of consumer protection class actions filed annually rose by about 156 percent.[36]

False Advertising Generally

Generally, the tapestry of laws covering false advertising consists of Section 5 of the FTC Act[37] (the "FTC Act"), Section 43(a) of the Lanham Act,[38] the state deceptive practices acts, and common law unfair competition. All of these laws target deception of one form or another, but they differ in their requirements as to who can bring an action, the burden of proof required, and the available relief.

Section 5 of the FTC Act prohibits "unfair and or deceptive acts or practices."[39] According to the FTC Policy Statement on Deception (1983),[40] deception exists if there is a material representation, omission or practice that is likely to mislead an otherwise reasonable consumer. Neither intent nor actual harm is a required element, and the FTC, in making a determination, is free to draw upon its experience and judgment rather from actual evidence in the marketplace.[41] The FTC will find an advertiser's failure to disclose facts actionable under Section 5 if a reasonable consumer is left with a false or misleading impression from

the advertisement as a whole.[42] The advertiser generally bears the burden of substantiating the advertising claim.[43] The FTC Act permits monetary and injunctive relief.[44]

Prior to, or in lieu of, an FTC proceeding, parties may find themselves before the National Advertising Division ("NAD"), a self-regulatory body that also focuses on resolving deceptive and misleading advertising. Parties generally participate in NAD proceedings willingly so as to avoid potentially more consequential action at the FTC. Although claims can be brought by consumers or competitors at the NAD, there is no private right of action at the FTC or in federal court under the FTC Act. Consumers seeking to file claims in court for consumer fraud and false advertising must resort to applicable state deceptive practices statutes and common law.

Competitors are also protected against deceptive practices under Section 43(a) of the Lanham Act, which provides for civil actions for injunctive and monetary (in state or federal court) for false or misleading statements made in commercial advertisement. The Seventh, Ninth and Tenth Circuit Courts of Appeals have tended to restrict standing under the Lanham Act to parties who are in direct competition; the other Circuits have a slightly broader standing threshold—but relief is not available to consumers. Under the Lanham Act, it is not necessary to show actual harm or intent to deceive to obtain an injunction.[45] To obtain damages, however, it is necessary to show that customers were deceived and that the plaintiff was harmed. Some courts raise a presumption of harm where the plaintiff proves the defendant's intent and bad faith.

The plaintiff in a Lanham Act action has the burden of proving that the claim is deceptive.[46] The Lanham Act prohibits false and misleading *statements*; accordingly, the mere failure to disclose or omission to state a fact is not per se actionable. However if the failure to disclose makes a statement "affirmatively misleading, partially incorrect, or untrue as a result of failure to disclose a material fact," then that statement is actionable.[47] In cases of implied deception, this means the plaintiff will have to introduce extrinsic consumer survey evidence.

As noted above, the growth of social media is likely to result in an increase in enforcement actions and private civil actions generally in connection with false advertising. Moreover, as discussed below, the FTC Guides make bloggers and advertisers using word-of-mouth marketing particularly vulnerable to deceptive practices and false advertising claims based on the blogger's failure to disclose a material connection to the advertiser.[48] In addition, to clarifying the FTC's own position with reference to how rules applicable to endorsements apply to social media, the FTC Guides are likely to be applied by state and federal courts when interpreting the Lanham Act and state deceptive practices acts.[49]

"Word of Mouth" Marketing

The Duty to Disclose

Social media has spawned virtually a new advertising industry and methods for spreading brand in an "old way": word-of-mouth marketing. Word-of-mouth marketing involves mobilizing users of social media to "spread the word" about the advertiser's goods and services. According to the Word of Mouth Marketing Association, word-of-mouth marketing is "[g]iving people a reason to talk about your products and services, and making it easier for that conversation to take place. It is the art and science of building active, mutually beneficial consumer-to-consumer and consumer-to-marketer communications."[50]

Word-of-mouth marketing typically refers to endorsement messaging. Specifically, an endorsement is "an advertising message" that consumers are likely to believe is a reflection of the opinions and beliefs of the endorser rather than the "sponsoring" advertiser.[51] When a television ad depicts "neighbors" talking about the merits of the Toro lawn mower, we don't believe that these statements reflect *their personal* beliefs; we know that they are actors speaking for the advertiser. On the other hand, Tiger Woods touting Nike golf equipment is an endorsement; we believe that we are listening to his personal views. A third-party's statement, however, is not an advertisement (and not an endorsement) unless it is "sponsored." In order to determine whether it is an endorsement consider whether in disseminating positive statements about a product or service, the speaker is: (1) acting solely independently, in which case there is no endorsement, or (2) acting on behalf of the advertiser or its agent, such that the speaker's statement is an 'endorsement' that is part of an overall marketing campaign?"[52]

As with all advertising, the bedrock concern of the FTC is with "unfair or deceptive acts or practices" prohibited under Section 5 of the FTC Act.[53] Deceptive acts or practices, generally, may include a failure to disclose material facts relative to a particular advertising claim. Thus, in the context of an endorsement, the relationship between the advertiser and the endorser may need to be made apparent to the consumer in order for the consumer to properly weigh the endorser's statement. The FTC Guides state that advertisers are subject to liability for false or unsubstantiated statements made through endorsements,

or for failing to disclose material connections between themselves and their endorsers, and that endorsers also may be liable for statements made in the course of their endorsements.[54] Section 255.5 of the FTC Guides requires that where a connection exists between the endorser and the seller that might materially affect the weight or credibility of the endorsement, such connection must be fully disclosed.

The FTC Guides distinguish three features of endorsements in the context of social media: (1) dissemination of the advertising message; (2) advertisers' lack of control; and (3) material connections.

First, in traditional print and broadcast media, the advertiser controlled the messaging. Endorsements were "embedded" largely in a message controlled by the advertiser. This has changed. As the FTC explains *(emphasis added)*:[55]

> When the Commission adopted the Guides in 1980, endorsements were disseminated by advertisers—not by the endorsers themselves—through such traditional media as television commercials and print advertisements. With such media, the duty to disclose material connections between the advertiser and the endorser naturally fell on the advertiser.
>
> The recent creation of consumer-generated media means that in many instances, endorsements are now disseminated by the endorser, rather than by the sponsoring advertiser. *In these contexts, the Commission believes that the endorser is the party primarily responsible for disclosing material connections with the advertiser.*

Consistent with this observation, the FTC Guides were amended to provide that "[e]ndorsers also may be liable for statements made in the course of their endorsements."[56] While at this writing the FTC has indicated that it does not intend to pursue individual users of social media and that it will be focusing enforcement on the advertisers, individual social media users would be ill advised to ignore the very clear mandates directed to them in the FTC Guides, standards that are also likely to influence courts in their interpretation of the Lanham Act and similar state laws.

Second, advertisers will frequently find themselves in relationships with apparently remote affiliate marketers, bloggers and other social media users. However, the advertiser's lack of control over these remote social media users does not relieve the advertiser of responsibility for an endorser's failure to disclose material information. "The Commission recognizes that because the advertiser does not disseminate the endorsements made using these new consumer-generated media, it does not have complete control over the contents of those statements."[57] The Commission goes on to state, however, that "if the advertiser initiated the process that led to these endorsements being made—*e.g.,* by providing products to well-known bloggers or to endorsers enrolled in word of mouth marketing programs—it potentially is liable for misleading statements made by those consumers."[58]

Importantly, for advertisers, the determination of liability hinges on whether the "the advertiser chose to sponsor the consumer-generated content such that it has established an endorser sponsor relationship."[59] Again, that relationship may exist with otherwise remote users. The FTC points out, however, that "[it], *in the exercise of its prosecutorial discretion, would consider the advertiser's efforts to advise these endorsers of their responsibilities and to monitor their online behavior in determining what action, if any, would be warranted.*"[60] To avoid prosecution, if not liability, advertisers should heed the Commission's admonition:[61]

> [A]dvertisers who sponsor these endorsers (either by providing free products—directly or through a middleman—or otherwise) in order to generate positive word of mouth and spur sales should establish procedures to advise endorsers that they should make the necessary disclosures and to monitor the conduct of those endorsers.

Finally, the FTC Guides indicate that social media endorsers may have a heightened duty to disclose material connections to the advertiser. "[A]cknowledg[ing] that bloggers may be subject to different disclosure requirements than reviewers in traditional media," the FTC states:[62]

> The development of these new media has, however, highlighted the need for additional revisions to Section 255.5, to clarify that one factor in determining whether the connection between an advertiser and its endorsers should be disclosed is the type of vehicle being used to disseminate that endorsement—specifically, whether or not the nature of that medium is such that consumers are likely to recognize the statement as an advertisement (that is, as sponsored speech). Thus, although disclosure of compensation may not be required when a celebrity or expert appears in a conventional television advertisement, endorsements by these individuals in other media might warrant such disclosure.
>
> . . . .

> The Commission recognizes that, as a practical matter, if a consumer's review of a product disseminated via one of these new forms of consumer-generated media qualifies as an "endorsement" under the construct articulated above, that consumer will likely also be deemed to have material connections with the sponsoring advertiser that should be disclosed. That outcome is simply a function of the fact that if the relationship between the advertiser and the speaker is such that the speaker's statement, viewed objectively, can be considered "sponsored," there inevitably exists a relationship that should be disclosed, and would not otherwise be apparent, because the endorsement is not contained in a traditional ad bearing the name of the advertiser.

Word of Mouth Marketing: Summary

The FTC's message is thus clear: (1) bloggers and other social media users are viewed as primary disseminators of advertisements; (2) endorsers in social media, along with the sponsoring advertisers, are subject to liability for failing to make material disclosures relating to the endorsement relationship (*e.g.*, gifts, employment and/or other connections and circumstances); (3) the FTC appears to take the position that there is a higher threshold of disclosure in social media than traditional media, and that the endorsement relationship itself is likely to trigger the obligation to disclose; (4) advertisers need to take reasonable steps to assure that material disclosures are in fact made; (5) advertisers cannot rely on the "remoteness" of the social media endorsers or on the advertiser's lack of control over them to escape liability; (6) advertisers are technically liable for a remote endorser's failure to disclose; (7) an advertiser's ability to avoid discretionary regulatory enforcement due to the endorser's failure to disclose will be a function of the quality of the advertiser's policies, practices and policing efforts. A written policy addressing these issues is the best protection.

False Endorsements

False endorsement cases arise under Section 43(a) of the Lanham Act where a person claims that his name or likeness, or actions attributed to him, are being used improperly to promote particular goods or services.

The Internet is rife with spoofing, fake profiling and other malicious conduct directed by one social media user against another. Frequently the conduct involves the transmission and publication of embarrassing or highly personal details about the victim. While historically, false endorsement cases have been brought commonly by celebrities or other people well-known to a community, the prevalence of social media will likely see the rise of false endorsement cases brought by non-celebrity victims under Section 43(a) and parallel state law.[63]

In *Doe v. Friendfinder Network, Inc.*,[64] the defendant operated a network of web communities where members could meet each other through online personal advertisements. Someone other than the plaintiff created a profile for "petra03755" including nude photographs and representations that she engages in a promiscuous lifestyle. Biographical data, according to the plaintiff, caused the public to identify her as "petra03755" to the community. The plaintiff alleged that the defendant did nothing to verify accuracy of the information posted, caused portions of the profile to appear as "teasers" on Internet search engine results (when users entered search terms matching information in the profile, including the true biographical information about the plaintiff,) and advertisements that in turn directed traffic to defendant's site. In denying the motion to dismiss the Lanham Act claim, the district court stated:[65]

> The plaintiff has alleged that the defendants, through the use of the profile in "teasers" and other advertisements placed on the Internet, falsely represented that she was a participant in their on-line dating services; that these misrepresentations deceived consumers into registering for the defendants' services in the hope of interacting with the plaintiff; and that she suffered injury to her reputation as a result....
>
> For purposes of this motion, then, the court rules that the plaintiff's claim for false designation under 15 U.S.C. § 1125(a)(1)(A) does not fail simply because she is not a "celebrity."

Defamation and Harmful Speech: Managing Corporate Reputations

In addition to confronting issues involving online brand management generally and word–of-mouth advertising specifically, corporations face similar challenges in protecting reputation, including risks associated with disparagement and defamation.

The architectures of the Internet and social media make it possible to reach an unlimited audience with a flip of the switch and a push of the send button—and at virtually no cost. There are few barriers to people speaking their mind and saying what they want. Furthermore, because of the anonymity social media allows, users are increasingly choosing to express themselves with unrestrained, hateful

and defamatory speech. These tendencies, encouraged exponentially by the technology and the near-zero cost of broadcasting one's mind, are likely to be further exacerbated under circumstances such as the current economic crisis, where people are experiencing extraordinary frustration and fuses are short.

Words can hurt. Defamation can destroy reputations. For individuals, false postings can be extraordinarily painful and embarrassing. For corporations, who are increasingly finding themselves victims of defamatory speech, a false statement can mean loss of shareholder confidence, loss of competitive advantage, and diversion of resources to solve the problem. While the traditional laws may have provided remedies, the challenges to recovering for these actions that occur over social media are enormous because the operators of the media that facilitate defamatory postings are frequently immune from liability. (Of course, if a corporation is the operator of a blog or other social media, there will be some comfort in the "immunities" offered to operators of these media.) The immunity under the applicable federal law, the Communications Decency Act (the "CDA"), and some other key issues associated with online defamation are discussed below.

Defamation Generally

Although the law may vary from jurisdiction to jurisdiction, to make a case for defamation, a plaintiff must generally prove: "(a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting at least to negligence on the part of the publisher; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[66] Defamation cases are challenging to litigate. It should be noted that in the United States, the First Amendment sharply restricts the breadth of the claim. Defamation cases frequently carry heightened pleading requirements and a shortened statute of limitations. If the victim is an individual and a public figure, he or she will have to prove malice on the part of the defendant to make a successful case. Finally, the lines between opinion and fact are frequently very hard to draw and keep clean.

Anonymous Speech

Online defamation presents added complications. Online, and in social media specifically, the source of the harmful communication is frequently anonymous or communicating through a fake profile. At the first line of attack, piercing anonymity of the anonymous speaker can be challenging because of heightened standards under First Amendment and privacy laws. A plaintiff victim will often file his case as a Jane or John "Doe" case and seek to discover the identity of the defendant right after filing. The issue with this approach is that many courts are requiring the plaintiff to meet heightened pleading and proof standards before obtaining the identity of the defendant. Effectively, if the plaintiffs can't meet the heightened pleading standard to obtain the identity of the defendant, they will be unable to pursue their cases. In one leading case, the New Jersey Appellate Court established a test that requires plaintiff "to produce sufficient evidence supporting each element of its cause of action on a prima facie basis," after which the court would "balance the defendant's First Amendment right to anonymous speech against the strength of the prima facie case presented and the necessity for the disclosure."[67]

Special Challenges: Service Provider Immunity

As noted above, the challenges to the corporate victim are compounded by the fact that its remedies against the carrier or host (the website, blog, search engine, social media site) are limited. The flipside, of course, is that corporations may have greater room in operating these kinds of sites and less exposure—at least for content that they don't develop or create. (*See Chapter 1 Advertising.*) A blogger will be liable for the content that he creates, but not necessarily for the content that others (if allowed) post on his blog site.

Early case law held that if a site operator takes overt steps to monitor and control its site and otherwise self-regulate, it might be strictly liable as a publisher for a third party's defamation even if the operator had no knowledge of the alleged defamatory content. Arguably, this encouraged site operators not to monitor and self-regulate.[68] Other early case law also held that if the operator knew about the defamation, it would be liable if it did not do something to stop the conduct.[69] These holdings arguably created an incentive to take down *any* potentially dangerous information to avoid liability—and thus, according to some, threatened to chill speech and dilute a robust exchange of ideas.

All of these early cases were overruled in 1996 by the CDA.[70] Section 230(c) of the CDA overruled all of the early cases by providing as follows: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[71] The term "information content provider" means "any person or entity that is responsible, in whole or in part, for the creation or

development of information provided through the Internet or any other interactive computer service."[72] Under Section 230(c), the operator, so long as not participating in the creation or development of the content, will be "immune" from a defamation claim under the statute.

The CDA makes it challenging to attach liability to a website, blog, social media platform or other electronic venue hosting offensive communication. Under U.S. law, these service providers have a virtual immunity, unless they participate in the creation or development of the content. Cases involving social media make the breadth of the immunity painfully clear. In *Doe v. MySpace, Inc.*,[73] a teen was the victim of a sexual predator as a result of conduct occurring on MySpace. The teen's adult "next of friend" sued MySpace for not having protective processes in place to keep young people off the social media site. In effect, the suit was not for harmful speech, but for negligence in the operation of MySpace. The Texas District Court rejected the claim, and in doing so highlighted the potential breadth of the "immunity":[74]

> The Court, however, finds this artful pleading [*i.e.*, as a "negligence" claim] to be disingenuous. It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe…. [T]he Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities. Therefore, in accordance with the cases cited above. Defendants are entitled to immunity under the CDA, and the Court dismisses Plaintiffs' negligence and gross negligence….

It is not clear that other courts would interpret the CDA as broadly as did the Texas court. Indeed, the breadth of the CDA remains highly disputed among the courts, academics and policymakers who raise the prospect of amending the law from time to time.

Companies that operate their own blogs or other social media platforms, such as a Twitter page can generally avoid liability for speech torts on their sites if they stick to traditional editorial functions—and do not allow those activities to expand into any conduct that could be interpreted as "creation and development" of the offensive conduct.[75] Although exercising editorial control is not penalized, the question confronting the courts is the point at which a company goes beyond editing or beyond providing a forum, and into the realm of *creation and development*.[76]

Where "creation and development" begins and ends may not always be a bright line. For example, the mere reposting of another "content provider's" content is arguably safe and within the editorial province of the social media operator. Although not completely free from doubt, it appears that a blog operator can receive a potential posting, review the content for editorial concerns, and then post it without the content thereby becoming the operator's creation.[77] Some courts hold that the operator's reposting to third-party sites is still within the grant of the immunity. In *Doe v. Friendfinder Network, Inc.,* for example, the community site caused the defamatory postings to be transmitted to search engines and advertisers and other linked sites. Holding that Section 230 protected that conduct, the court noted: "Section 230 depends on the source of the *information* in the allegedly tortious statement, not on the source of the statement itself. Because 'petra03755' was the source of the allegedly injurious matter in the profile, then, the defendants cannot be held liable for 're-posting' the profile elsewhere without impermissibly treating them as 'the publisher or speaker of [ ] information provided by another information content provider.' … 47 U.S.C. § 230(c)(1)."[78]

Plaintiffs continue to reach for creative attacks on Section 230. In *Finkel v. Facebook, Inc., et al.*,[79] the victim of alleged defamatory statements claimed that Facebook's ownership of the copyright in the postings barred its right to assert Section 230. The plaintiff urged, in effect, that the defendant could not claim ownership of the content and simultaneously disclaim participation in the "creation and development" of that same content. Rejecting this argument, the New York trial court stated that "'[o]wnership' of content plays no role in the Act's statutory scheme."[80] Furthermore, the court reiterated Congressional policy behind the CDA "by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others."[81] The court was clear in dismissing the complaint against Facebook where the interactive computer service did not, as a factual matter, actually take part in creating the defamatory content.

This is an important decision. Many sites assume ownership of content through their terms of use, and a contrary ruling would materially restrict application of the CDA in those cases. Further litigation is likely in this area.

Some courts have explored plaintiffs' assertions of service provider "culpable assistance" as a way of defeating the provider's CDA defense. In *Universal Comm'n Sys., Inc. v. Lycos, Inc.*,[82] the plaintiff argued that the operator's immunity was defeated by the construct and operation of

the website that allowed the poster to make the defamatory posting. The First Circuit rejected the argument for a "culpable assistance" exception to the CDA under the facts as presented, but left open the possibility of such an exception where there was "a clear expression or other affirmative steps taken to foster unlawful activity."[83]

This result is consistent with the Ninth Circuit's decision in *Fair Housing Council of San Diego v. Roommates.com, LLC*.[84] In that case, involving an online housing service, the court held that the CDA did not provide immunity to Roommates.com for questions in an online form that encouraged illegal content. Roommates.com's services allowed people to find and select roommates for shared living arrangements. The forms asked people questions relating to their gender and sexual orientation. Although Roommates.com clearly did not provide the content in the answers, the Ninth Circuit held that it was not entitled to immunity. The majority ruled that Roommates.com was not immune for the questionnaire itself or for the assembling of the answers into subscriber profiles and related search results using the profile preferences as "tags." The court noted that the questions relating to sexual preferences posted by Roommates.com were inherently illegal and also caused subscribers to post illegal content themselves by answering the questions. In a case that evoked a sharp dissent and defense of a strong immunity, the clear take-away from the *Roommates.com* decision is a view that the immunity is far from absolute.[85]

Entities that operate social media sites need to be especially careful not to allow their "editing" to turn into creation and development of content. Although these issues are far from settled, any embellishments and handling of posted content should be approached cautiously and only in the context of traditional editorial functions.

CDA Immunity: Scope of the IP Exception

One important issue dividing the courts is the scope of the immunity as it relates to intellectual property. Specifically, although the CDA confers a broad protection on service providers, it also provides that it "shall [not] be construed to limit or expand any law pertaining to intellectual property."[86] In other words, a blog operator, for example, cannot assert a CDA defense to claims that, although involving speech, are rooted in harm to the victim's intellectual property. If the victim asserts, as against the operator a claim for copyright infringement based on a blogger's uploading of protected material on to the blog (clearly involving "speech"), the operator has no CDA defense. The victim and the operator will have to resolve their claims under the copyright law, and particularly the Digital Millennium Copyright Act. Likewise, if the victim asserts a claim under Section 1114 of the Lanham Act that its federally registered trademark is being wrongfully used on the blog, the operator arguably cannot rely on the CDA as a shield against liability.[87]

The courts differ over the scope of the intellectual property exception to immunity, and specifically over the definition of intellectual property for purposes of the statute. In *Perfect 10, Inc. v. CCBill*, LLC,[88] the court opted for a narrow reading of "intellectual property" and hence a broader scope for the immunity. Specifically, the Ninth Circuit "construe[d] the term 'intellectual property' to mean 'federal intellectual property.'"[89] Accordingly, without determining whether the state law claims truly involved "intellectual property," the Ninth Circuit held that the intellectual property exception does not, as a threshold matter, apply to state law claims, and therefore affirmed dismissal of various state law claims on CDA grounds.

On the other hand, some courts have opted for a broader reading of "intellectual property" that would have the exception cover relevant state law. For example, the court in *Doe v. Friendfinder Network, Inc*. determined that intellectual property under the CDA exception encompasses applicable state law and, on that ground, refused to dismiss the plaintiff's right of publicity claim against the website operator.[90]

Reporter's Privilege

Application of existing rules to new technologies can raise yet more hurdles in speech cases. For example, suppose false information about your company appears on a blog or that some bit of confidential information appears. As part of damage control, you may want to find the source–or compel the blog to disclose the source. This leads to an interesting question–to what extent are blogs actually "newspapers." The question is one that courts are being forced to consider, because newspapers traditionally have a "reporter's privilege" that allows them to resist revealing their sources. For example, in 2004, Apple faced such an issue with respect to someone who allegedly leaked information about new Apple products to several online news sites. Apple sought the identity of the site's sources and subpoenaed the email service provider for PowerPage, one of the sites, for email messages that might have identified the confidential source. In 2006, a California Court of Appeals provided protection from the discovery of sources by the constitutional privilege against compulsory disclosure of confidential sources.[91] Courts continue to consider similar issues, and a number of legislative proposals have been introduced at the state and federal level.

Bottom Line—What You Need to Do

Clients who are victims of speech torts must be prepared to act—but they must use the right tool when the problem arises. These tools range from a conscious choice to do nothing, responding with a press release; responding on the company's own blog, fan page on Facebook and/or Twitter page; and/or engaging a reputation management company (for example, making use of search engine optimization techniques to reduce visibility of negative comment). The negative publicity associated with disparaging comments can be greatly exacerbated by "sticky" sites that get high rankings on Google causing, for example, a negative blog posting to be highly listed when a potential customer types your organization's name into Google or another search engine. Your organization is well advised to undertake a multi-prong strategy: consider the legal options, but consult with search engine and reputation management specialists to see if there might be a communications/ technical solution. Of course, litigation, including proceedings to unmask the anonymous speaker, should be considered. But a heavy-handed approach may simply make a bad situation worse—and at great expense. Litigation—or even a cease-and-desist letter that finds its way to an Internet posting—may give your organization exactly the kind of publicity it does not want.

Frequently, malicious actors will time their communications to a key corporate event, such as the company's earnings reports, in order to enhance the damage from the comment. Gone are the days when response to an incident can be vetted by a formal legal memorandum to corporate counsel. The damage can be "done" in literally a matter of hours. A quick response can make all the difference.[92] Accordingly, it is important for companies to understand the exposures to brand and reputation in social media, to have policies in place for managing internal and external communications in these new media, and to have contingent plans for dealing with reputation and brand disparagement, whether as the responsible party or as the victim, before the event happens—so that the response can be quick and damage the minimal.

— CHAPTER 3 —

Data Privacy & Security

Chapter Authors

Paul Bond, Associate – pbond@reedsmith.com

Amy S. Mushahwar, Associate – amushahwar@reedsmith.com

Introduction

This chapter explores the implications in social media arising from the laws and regulations surrounding data privacy, security and information security management.

According to statistics published on Facebook,[93] there are more than 300 million active users of Facebook worldwide, and more than 120 million users log onto the site at least once each day. Most major brands have Facebook group and/or fan pages—with commentators even doing case studies of those that have been most effective.[94] Yet, there remains a reluctance by some companies and brands to use social media. Social networking sites such as Twitter, MySpace, Facebook and LinkedIn may enhance collaboration and help companies connect with customers, but they can also make it easier than ever for employees and customers to share confidential customer data, company secrets and negative product information. A major airline's Valentine's Day debacle exemplifies how the usefulness of social media is tempered by fear of what might be disclosed.[95] The passengers were stranded on the tarmac, some up to 11 hours, while a rapidly moving storm tore through the East Coast. Passengers were immediately on their cell phones and stories accompanying pictures of overflowing toilets instantaneously appeared in social media. Just as this incident spread virally via social media, so too might the liability associated with a breach of protected information. Millions of dollars in claims could be made against the hosting site and cause both the bad press and the legal damages that can add up to millions.

Social Media in Action in Data Privacy & Security

Personal data collected by social media companies is at risk from all sides. Thieves want to profile, steal and resell personally identifiable information and data. Employees are tempted to misuse customer data, for monetary gain or to satisfy idle curiosity, perhaps with no malicious purpose at all.[96] Even standard business processes pose risks to personal data. Social media enterprises collect, store, use, share, and dispose of personal data every day, including eCommerce-related non-public financial information (*e.g.*, credit, banking and payment information). Each of these inflection points is an opportunity for something to go wrong, for a law to be broken or a data subject put at risk. Here are some things social media companies and companies that use social media should know.

Company Obligations Set Forth in the User Agreement

User agreements are private agreements between the publisher and its users, and they define the rights and obligations of each party. Typically, user agreements have at least two components: (1) a privacy policy and (2) a terms of use. While there is no legal distinction between putting them into one document rather than splitting them, social media and web-based services recognize the increased importance privacy and data protection play—not only in law and regulation, but also to consumers. Creating a separate document, page or display makes these terms conspicuous, and in a visual and distinctive manner create a better "notice and disclosure" or so-called transparency argument, should a consumer or a regulator challenge the efficacy of notice to consumers. Privacy policies are statements made by companies about their practices regarding personal information. Companies on

the Internet, social media or otherwise, post privacy policies to disclose information practices in accordance with federal and state statutes.[97] Terms of use, on the other hand, describe the terms and conditions governing the relationship between the user and the publisher or operator of the service. Because privacy policies are effectively part of the terms and conditions—the rights and obligations—between the parties, we may simply refer to them as the "agreement" in these materials.

Because these agreements run between and among publishers and users (and sometimes a company that is using a service or website), a company's obligation with respect to personal data will change depending upon whether it is the social media service (*e.g.*, Facebook, MySpace or Twitter), a company-sponsored fan site (*e.g.*, a Starbucks sponsored fan site on MySpace) or an unrelated third-party fan site.

Social Media Companies

Social media companies, as authors of these agreements, have the primary responsibility to ensure all personally identifiable information that is collected, used, stored and shared, is used in accordance with the user agreement (and, of course, law and regulation). But, this does not mean that social media companies must be overly conservative in their user agreements. Most social media companies do not charge any recurring user fees for use of their web site. So, access to and data from users in the web site community is a social media company's primary commodity to monetize the site.

The need for information monetization can create in an adversarial relationship between the site user and the social media company. As a result, many consumer advocacy organizations are analyzing and notifying consumers of updates to social media website user agreements.[98] These consumer watchdog organizations can generate considerable controversy; take for example, Facebook's recent Terms of Service update. In February 2009, *The Consumerist* flagged a series of changes to the Facebook Terms of Service, including deletion of the following text:[99]

> You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.

From this deletion, *The Consumerist* author, Chris Walters, opined that: "Now, anything you upload to Facebook can be used by Facebook in any way they deem fit, forever, no matter what you do later," Walters wrote. "Want to close your account? Good for you, but Facebook still has the right to do whatever it wants with your own content." Ultimately, *The Consumerist* blog created a firestorm, which caused Facebook to repeal its Terms of Service changes three days after the blog was posted.

But, the Terms of Service change is not the only example of the tension created over the use of consumer information and consumer disclosures. In November 2007, Facebook launched its Beacon advertisement system that sent data from external websites to Facebook, ostensibly for the purpose of allowing targeted advertisements. Certain activities on partner sites are published to a user's News Feed. Soon after Beacon's launch, civic action group, MoveOn.org, created a Facebook group and online petition demanding that Facebook not publish their activity from other websites without explicit permission from the user.[100] In less than ten days, this group gained 50,000 members. Beacon amended its user agreement policy, as a result.[101] A class action lawsuit was filed against Facebook as a result of Beacon. The lawsuit was ultimately settled in September 2009[102], and the Beacon advertisement service was shutdown.

Company or Third-Party Sponsored Fan Site or Portal

Many companies, however, do not own or operate a social media website, and thus, do not author the social media user agreement. Instead, these companies are monitoring content regarding their products and services on fan sites/portals run by another company. For example, Starbucks does not operate its own social media website, but operates portals on MySpace, Facebook, Twitter and YouTube. The key for removing portal information is to know where the content lies (on a company or third-party sponsored portal), and the user agreement of the social media website the offending information lies upon.

For portals or fan sites that are sponsored by the marketing company, it is simple for the company to remove offending information. Facebook, MySpace and YouTube offer page administration options for content removal on company-sponsored portals. For these services, the company can directly control content posted to the portal by designating in its administrative options to pre- or post-screen user-generated content. Twitter, however, works differently. On the company-sponsored Twitter profile, the company can control what "Tweets"[103] it sends to its followers, but the company cannot directly control what is "retweeted"[104] by others from the company-sponsored tweets.[105]

For portals or fan sites that are third party in nature, it is more difficult to administer content and remove known

privacy violations. Removal of third-party content involving your company or brand is governed by the respective social media website's user agreement, all of which are different. Take, for example, if one of your employees records a confidential session (a health care visit, tax preparation, loan application meeting, etc.) between the employee and one of your customers. Could the company seek removal of the confidential video? The question of whether a corporation could remove this content on behalf of its customer is different depending upon what social media service is used.

- On YouTube the answer is no. On YouTube, the remedy for removing content is flagging it for removal. Under the YouTube privacy policy, YouTube will not permit privacy flagging on behalf of other people.[106] Alternatively, companies could issue cease-and-desist e-mails directly to the YouTube content poster.
- On Facebook the answer is possibly. On Facebook, the remedy for removing content is reporting poster abuse of Facebook's Statement of Rights and Responsibilities (the "Terms").[107] In Section 5 of the Terms, Facebook will not permit posting of "anyone's identification documents or sensitive financial information on Facebook."[108] Depending on the content of the private information disclosed in the video-taped confidential meeting, a company could report a violation on behalf of its customer.
- On MySpace the answer is yes. On MySpace, the remedy for removing content is submitting a request to delete inappropriate content that violates the website's Terms of Use Agreement.[109] Under the Terms of Use Agreement in Section 8, any postings that would violate the privacy and/or contractual rights of another party are prohibited.[110] In this scenario, there would be both an individual privacy right on behalf of the customer and a contractual confidentiality right of the company (provided a proper confidentiality provision is in place with the employee).

Notwithstanding the contractual user agreement rights and obligations on social media, a number of national and international laws also govern this area.

Company Obligations Set Forth in National and International Law

Today, businesses operate globally, with technology that knows no national boundaries. Nothing comes more naturally than sharing and sending information halfway around the world. Social media epitomizes that modern, global ethos.

But every jurisdiction in the world can claim the right to protect its citizens–and information about them. The United States has a very different conception of "personal information" and adequate protection of it than does the European Union; the EU view does not necessarily speak for all of its member States; and some of those States have their own local standards. And so it goes, in every part of the world.

A social media company can be completely compliant with United States law and still run afoul of legal mores elsewhere. Notably, the EU's Article 29 Data Protection Working Party has set forth an opinion on online social networking.[111] This Opinion, adopted June 12, 2009, opines that "social networking services" or "SNS" are generally data controllers, and SNS subscribers are generally data subjects. In the view of these authors, even those SNS located outside the EU are bound to respect EU strictures on data processing and onward transfer as to residents of EU member countries. Where a subscriber's information is only available to a self-selected circle of friends, the Opinion posits that the exception allowing sharing of personal information within households applies. But when access to the subscriber's information is shared more broadly, with or without that subscriber's consent, "the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web."[112] The Working Paper goes on to state a number of other positions regarding marketing by SNS, complaint procedures, and (advocating) the availability of pseudonyms.

Facebook experienced a culture clash with Canada's privacy commissioner with respect to the disposal of personal information. Facebook had been retaining data on subscribers who quit, so that they could more easily rejoin should they choose to do so later. Canada's privacy commissioner determined that Facebook's retention of data was a violation of Canada's Personal Information Protection and Electronic Documents Act, and negotiated a settlement that provides that, "Collected personal information can be kept only for a specified time and must be deleted or destroyed when no longer needed."[113]

The Next Direction in Privacy Law [114]

The main challenge for social media companies is that the regulatory privacy obligations seem to be developing on-the-fly in this area. There was no law clearly forbidding Facebook from partnering with several dozen other sites to

share information regarding subscriber usage of affiliate sites. There was no law clearly forbidding Facebook from making such activity logs visible to the subscribers' friends. Facebook even provided a pop-up, opt-out mechanism to help respect subscriber privacy choices. Yet following a class action lawsuit, discussed above, Facebook is shutting down its Beacon program and donating $9.5 million to a nonprofit foundation to promote online safety and security.[115] Clearly, as important as existing laws are the developing sensibilities of both consumers and privacy officials. The predominant theme appears to be a profound antipathy toward the aggregation and use of information of consumer behavior, however well disclosed. Social media companies need to proceed very carefully in capitalizing on the wealth of information that they are assembling, developing subscriber and policymaker support for programs in the works, and adequately disclosing program information to consumers, at a minimum, in the user agreement. Moreover, companies need to realize that even where the law has been slow to catch up, consumer reaction and the threat of regulatory or legal action has often shaped privacy practices in social media. Keeping on top of those trends is critical.

Take, for example, the 2009 industry initiative to address concerns over behavioral advertising. In 2009, the American Association of Advertising Agencies, Association of National Advertisers, Interactive Advertising Bureau, Direct Marketing Association and the Better Business Bureau, completed a joint business initiative and released the "Self-Regulatory Principles for Online Behavioral Advertising".[116] The trade groups worked closely with the Council of Better Business Bureaus in crafting the principles. The initiative was in response to urging by the Federal Trade Commission that unless the industry adopted polices, government regulators would step in.

The industry effort covers the categories the Federal Trade Commission identified as the key areas of concern: education, transparency, consumer control, data security, material changes, sensitive data and accountability. The Council of Better Business Bureaus, along with the Direct Marketing Association, are now developing additional policies to implement accountability programs to give some teeth to the self-regulatory rules and to foster widespread adoption of the principles.

Company engagement in (or Avoidance of) Third-party Legal Disputes

Increasingly, information gathered by social media sites is at the center of legal controversies to which social media companies themselves are strangers.

- Social media sites are routinely used for sting operations seeking out sexual predators.[117]
- On the other hand, one criminal defendant in a forcible rape case tried to enter into evidence the victim's Facebook status page. He claimed that this social media showed that the victim's complained-of bruising resulted from heavy drinking on other occasions.[118]
- A Canadian court allowed discovery of a Facebook profile in a motor vehicle accident suit, despite the document being subscriber-designated as limited access.[119]
- If an employer terminates an employee for cause, recommendations that the employers had made regarding that employee on a site like LinkedIn may be evidence of pretext.[120]
- Subscribers' posts may violate their own company's privacy policies, or even reveal their own company's trade secrets.[121]
- Subscribers may later regret their social media postings, but the evidence that those posts were made can be crucial. One MySpace subscriber posted an article heavily critical of her hometown. Six days later she removed it. But, in the meantime, it had been republished in her hometown newspaper arousing the ire of her community to the extent her family had to close its business and move. The subscriber sued the paper who republished the article. The court held that the initial MySpace publication made any subsequent republication fair game, and non-actionable.[122]
- Presenting perhaps even additional complications, courts in some countries, like New Zealand and Australia, have allowed official court process to be served over social medial sites.[123]

Both the social media enterprise and individual companies on social media can protect themselves. As stated above, each social media enterprise already has (or should have) a detailed suite of policies, reflected in the user agreement, to determine how the company fits in to the substance and process of third-party legal actions. Likewise, all companies should put policies in place governing employees' actions on social media to avoid company vicarious liability.

Protections to Deter Criminal Activity

Data security class action litigation usually focuses not on the (often judgment-proof) criminal wrongdoers themselves, but on the companies those wrongdoers happened to work for, with, or through. Moreover, governments around the world have drafted businesses

into the war against identity theft. Hefty fines can result from a lack of due diligence.

In social media enterprises, an even greater risk than identity theft or financial fraud exists. Users of social media have been exposed to emotional abuse[124] and have been sexually assaulted,[125] among other crimes. Attempts have been made to hold the social media enterprises themselves liable for not doing more to stop these abuses. While legal actions have generally not resulted in recovery against social media enterprises, the attendant bad publicity and subscriber concern carry a cost of their own.

Where there is a pre-existing protective order in place, even the simple act of making a friend request via a social media service can rise to the level of criminal contempt.[126] And, especially where the social media environment involves the creation or accumulation of some artificial currency, subscribers can also abuse the system to achieve property crimes or tax evasion.[127]

Precautions to detect likely criminal activity, to the extent practicable, and having social media employment agreements to establish company expectations, are essential for any business's self-preservation. Typically, companies can take actions such as routine audits and establishing human resources notification policies for crimes involving employees in the workplace. Social media employment agreements are now essential for individuals doing work for your business. We recommend evaluating all of the types of individuals employed by your company and developing a social media agreement that will fit for: employees, contractors, hired talent (representing the company in an endorsement/marketing context), and outsourcing contracts, where applicable. (*See Chapter 4 Employment.*)

Addressing Traditional Data Security Concerns

Every social media enterprise needs a comprehensive written information security program. The very open architecture that allows social media enterprises to thrive also allows information security threats to multiply. For example, the Twitter worm, "StalkDailey," "can gain access to unsuspecting Twitter users by masquerading as the family, friends, and co-workers of the user."[128] In fact, 19 percent of all hacking attacks were directed at social media enterprises in the first half of 2009, "ranging from simple defacement of sites, placing malware on them or using them to spread smear campaigns."[129] Social media enterprises need to enlist not just their employees, but also their subscribers, in rapid response to developing privacy threats based on well-understood policies and procedures. Failing to do so may result in dilution of a brand's value as regulators and consumers react to lapses in security.

A written policy is necessary, but not sufficient to ensure compliance. A written policy without implementation and adherence is a dead letter. Plain language review, easy-to-follow training materials, employee testing, vendor auditing, security breach drills, and the like are indispensible to making sure policy is part of day-to-day procedure.

At the same time, outreach to subscribers to let them know what to expect (and not expect) from the company will help subscribers defend themselves from spoofers, phishers, and similar would-be attackers.

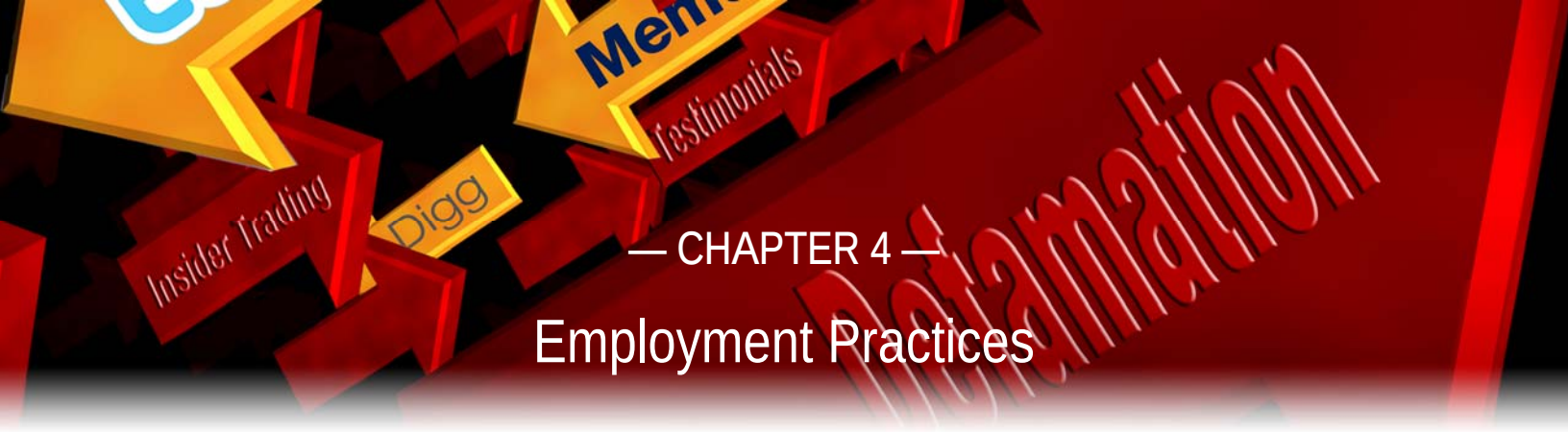
Also, like every company, social media companies should have plans for: the protection and secure disposal of personal data (including in hard copy); the implementation of major litigation holds; and response to the loss or theft of personal data (including, where required or appropriate, through notice to data subjects).

Is the company properly insured against data privacy incidents?

The last risk you need to plan for is the risk that all other mitigation will, ultimately, not be sufficient. As noted above, no system is perfect. Data privacy and security lawsuits can cost millions or tens of millions of dollars to resolve. The right level of coverage, either under general policies or specific endorsements, is something that every company needs to determine on an ongoing basis.

Bottom Line—What You Need to Do

Understand the sensitive nature of information that flows through social media. Recognize the serious compliance and litigation risks that the collection and distribution of such information entails. Consider contractual tools to mitigate these risks, including properly drafted privacy policies and terms of use. Know your obligations under all applicable data privacy and security laws, and have a nuts-and-bolts plan to meet those obligations. Stay ahead of developments in data and privacy security law, so that, to the extent possible, the compliance program put in motion today will be deemed adequate even under the standards of tomorrow. Lastly, know your coverage position with respect to data privacy and security incidents, and properly adjust that coverage in light of known and suspected risks.



— CHAPTER 4 —

Employment Practices

Chapter Authors

Casey S. Ryan, Partner – cryan@reedsmith.com

Amber M. Spataro, Associate – aspataro@reedsmith.com

Introduction

This chapter looks at the relationship between social media and employment practices. The interplay between the use of social media and employment law is fraught with unknowns. Social media is a boon in every facet of employment from hiring and firing to marketing and business development. At the same time, such use not only engenders legal risks, but reputational and public relations risks as well.

Recent surveys have found that approximately 60 percent of employees either do not know if their employer has a social media use policy or believe that their employer does not.[130] A Deloitte LLP study found that 74 percent of employees surveyed agree that it is easy to damage a company's reputation on social media.[131] By June 2009, the number of employers who had terminated an employee for conduct related to his/her use of a social media site doubled to 8 percent, compared with only 4 percent in 2008.[132]

Currently, the law with respect to employment and social media is practically devoid of any useful guidance for companies. Instead, employers must rely upon basic principles related to employee privacy, anti-discrimination and harassment law, intellectual property law and other applicable law, in order to discern how to best use (and control the use of) social media in the workplace.

Social media can be used by companies in a variety of employment aspects, such as in the hiring process or in discovering fraudulent workers' compensation claims. It may also serve as a strong recruiting tool and connection between potential employees and the company.

On the other hand, employee use of social media may be devastating to a company, both legally and from a public relations perspective. Social media may serve as a setting for the type of employee banter that, if used in the workplace, would violate an employer's anti-harassment or other policies. Moreover, social media is an outlet for an employee to "gripe" about his or her employer and possibly damage the employer's reputation. At worst, social media may be used by employees, whether intentionally or not, to divulge trade secrets, or copyright-protected or other confidential company information.

This chapter provides companies with an overview of how social media affects the workplace and the issues to consider and manage regarding the circumstances under which a company or its employees use social media. We begin by examining the possible uses of social media by employers and then turn to use by employees, and finally a discussion of how a company can seek the removal of content posted by employees in social media.

Social Media in Action in Employment

Employer Use of Social Media

Does your company have a company-sponsored page on one or more social media sites? If so, what do you use it for? Many large multi-national companies create pages on social media sites and use them for everything from marketing promotions (*See Chapter 1 on Advertising and Marketing)* to seeking job applicants. Such uses are arguably the most acceptable and productive for a

company. However, to minimize legal risk, such sites should be properly and consistently monitored for derogatory content and posts and, if such content is posted, it should be promptly removed. Since the company controls the site, such removal is a fairly simple process.

Does your CEO have a Facebook or other social media page(s)? Should he/she? Sometimes, a CEO may create his/her own social media page in order to market the company. Other times, such sites may be strictly personal and have nothing to do with the company, other than its reference as his/her employer. It is sometimes difficult to discern whether a CEO's social media page was created in his/her capacity as CEO or as a personal outlet. (*See Section B, below, regarding employee use of social media.)*

Does your Human Resources department use social media as a recruiting tool or to investigate the credentials and qualifications of job applicants? How about to keep track of the activities of current employees? If so, the legal parameters for such use have not yet been resolved. Employers must be cognizant of the possible privacy rights at stake, as well as possible issues related to compliance with the Fair Credit Reporting Act.

Similarly, an employer may use social media to ferret out fraudulent claims for workers' compensation or unemployment benefits. Insurance carriers have been increasingly using social media sites to expose claimants supposedly too injured to work, but who are engaging in sports competitions or other physical endeavors.[133] Employers may possibly be able to do the same.

Employee Use of Social Media

Do some or many of your employees have social media pages or spaces? If so, do they visit them at work? During working hours? Using company equipment? In such situations, an employer may and should be able to lawfully restrict and/or limit an employee's use of social media. With properly worded notice to employees, an employer has practically an unfettered right to control the use of its own property, such as computers, cell phones, and PDAs. Similarly, if proper notice is given, employers may also monitor the use of the company's property without restriction.

With respect to on-duty use of social media, an employee's time on the clock belongs to the employer and, thus, an employer may properly restrict or limit an employee's use of social media while on duty, even if the employee is using personal equipment. However, if an employer permits on-duty use of social media when an employee uses his or her own equipment, the employer generally may not use electronic means to observe or monitor that use, but may be able to police the use to the extent that it impacts the workplace, either by reduced productivity or by conduct that may expose the employer to liability.

Social media sites can be, and are often used as, communication tools between employees. However, at times, the content of those employee communications may cross the line into harassing, threatening or other unlawful conduct, or divulge trade secrets or other confidential information about the employer or a competitor. In such a situation, it is an open question whether an employer may be held legally liable for damages resulting from the offending employee's post.[134]

Accordingly, the next question is whether an employer can or should use content posted on social media sites as a basis for disciplining or discharging an employee. Notably, content posted anonymously is very difficult to police and several states have laws prohibiting employers from taking adverse action against an employee for engaging in lawful, off-duty conduct. Moreover, employers must be cautious about taking adverse action against any employee whose social media use could be construed as protected, concerted activity pursuant to the National Labor Relations Act ("NLRA"), no matter how derogatory the post may be to the company. Finally, government employers have the additional concern of possibly violating their employees' First Amendment rights by disciplining an employee for content he/she posted on a social media site.

On the other hand, employers cannot turn a blind eye to their employees' use or abuse of social media sites. Consequences of doing so include loss of confidential information and/or trade secrets; reputational harm to the business, either through the employee's misconduct or the appearance that the company condones or adopts the employee's statements; and possible legal liability of the employer for employee content that is defamatory, threatening or otherwise unlawful.

Recently, the FTC revised the Guides Concerning the Use of Endorsements and Testimonials in Advertising[135]. It is unclear to what extent, if any, an employer may be liable for an employee's statements in social media; however, the FTC provides an illustrative example in Part 255.5 that indicates that both employers and employees may be liable in some circumstances. Under Example 8 of 16 C.F.R. Part 255.5, an online message board designated for discussions of new music download technology is frequented by MP3 player enthusiasts… Unbeknownst to the message board community, an employee of a leading

playback device manufacturer has been posting messages on the discussion board promoting the manufacturer's product. Knowledge of this poster's employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board. 16 C.F.R. Part 255.1(d) provides that "[a]dvertisers are subject to liability for…failing to disclose material connections between themselves and their endorsers. Endorsers also may be liable for statements made in the course of their endorsements." Therefore, in Example 8, both the employee and the employer may be liable for the employee's failure to disclose his material connection with the employer.

Removing Content Posted by Employees from the Site

If an employee uses social media to post derogatory, defamatory, harassing, threatening, confidential or other unlawful or inappropriate content, what can the company do to get such content removed from the social media site?

Most social media sites have terms of use that prohibit the posting of any content which is threatening, harassing, defamatory or otherwise unlawful. Presumably, then, any such content would be voluntarily removed by the site after it is brought to the site's attention.[136] However, not all sites prohibit the posting of content that may constitute confidential information, but that is not copyrighted or may not rise to the level of a trade secret or other legally protected information.

For example, MySpace's terms of use prohibit the posting of any content that "violates or attempts to violate the privacy rights, publicity rights, copyrights, trademark rights, contract rights or any other rights of any person."[137] However, Facebook does not appear to share this same view. Facebook's terms of use only prohibit the posting of content that "infringes or violates someone else's rights or otherwise violates the law."[138]

Accordingly, if an employer complains to Facebook that a post discloses confidential information pertaining to the company, but cannot show that the information is legally protected, it is an open question whether Facebook will remove the offending post. Indeed, currently, no laws would *require* Facebook to remove such a post.

Current Legal and Regulatory Framework in Employment

Little case law exists pertaining to employee use or abuse of social media, and there are no statutes or regulations that would specifically govern such conduct. Currently, an employer's management of its and its employees' use of social media must be guided by the basic principles related to employee privacy rights and protections, anti-discrimination and harassment law, intellectual property law, free speech concerns, and other applicable law.

The role of intellectual property law in social media is fairly straightforward and an employer should not be inhibited in any way from policing or enforcing its right to protect its intellectual property from being exploited on social media sites. However, anti-discrimination and harassment laws, laws protecting an employee's right to engage in lawful off-duty conduct, privacy rights and other concerns such as free speech rights, play a larger role in shaping how an employer may use, or control its employees' use of, social media.

Arguably, an employer could always prohibit its employees from posting any content on social media that constitutes unlawful harassment or discrimination. Title VII of the Civil Rights Act of 1964 and amendments thereto,[139] as well as numerous state laws, prohibit harassment of employees by other employees based on certain protected characteristics. However, the question of what type of conduct constitutes harassment based on a protected characteristic and whether such conduct is sufficiently severe or pervasive to be unlawful is always a difficult one. To further complicate the issue, several states prohibit employers from taking adverse action against an employee who is engaging in lawful, off-duty conduct.[140] Accordingly, it is unclear whether an employer may, for example, lawfully discipline an employee for posting, on his or her own time and equipment, sexist or racist jokes on his or her MySpace page.

By the same token, no case law has yet determined the circumstances (if any) under which an employer could or would be held vicariously liable for an employee's alleged harassment by another that occurs on a social media site. Nevertheless, in the Title IX context (which prohibits harassment of students on the same bases and imposes liability for such harassment on schools in certain circumstances), parents have sought to hold schools liable for, *inter alia*, the use of Facebook and other social media sites to "sexually harass" their children.[141] However, since the cases also included numerous other types of alleged harassment, such as face-to-face confrontations, etc., it is

difficult to tell what role, if any, the content on Facebook played in determining whether the school did (as in one case) or did not (as in the other) have any liability for the alleged harassment.

Another example of an area where an employer must use caution is whether to prohibit and/or discipline employees for social media content that could arguably be construed as "protected, concerted activity" under the National Labor Relations Act[142] regarding working conditions, even if such content is derogatory to the company and/or other employees. Employee privacy rights may also play a role depending upon the circumstances under which the employer became aware of the offending conduct. Finally, government employers must consider their employees' First Amendment rights if the scope of their employees' prohibited use of social media arguably affects an employee's right to speak on an issue of public concern.

Bottom Line—What You Need to Do

If your company has not developed policies for use of social media by your employees, now is the time to act. A properly drafted policy on the use of social media by employees is an employer's most effective tool in protecting itself against legal liability and harm to its reputation and good will from the use of social media.

In most cases, a properly drafted policy pertaining to employee use of social media should assist an employer in protecting its interests. However, policies are not one-size-fits-all. They must be tailored to the culture, needs and realities of your specific workplace.

Some elements to consider in creating and implementing a social media use policy include: (1) the company's level of tolerance for personal use of social media; (2) whether the company should permit or even require use of social media for marketing and business development; (3) how the company will handle employees who post arguably inappropriate, but not unlawful, posts such as illicit photos, profanity or other potentially derogatory content; (4) how the company will comply with laws protecting employees' right to engage in lawful off-duty conduct, but still ensure nothing damaging is posted online; (5) once the policy is in place, how the company will train employees so they understand what is forbidden (for example, one person's definition of "crude" may vary from another's); (6) how the company will monitor compliance with and enforce the policy; and (7) what the repercussions will be for violations.

Employees need guidance in their use of social media: every employer should have such a policy in its Employee Handbook, and strictly monitor and enforce compliance or face exposure to currently unknown legal or professional risk.

— CHAPTER 5 —

Government Contracts & Investigations

Chapter Authors

Andrew L Hurst, Partner – ahurst@reedsmith.com

Daniel Z. Herbst, Associate – dherbst@reedsmith.com

Introduction

This chapter looks at the relationship between social media, government contractors, and those businesses regulated by the government or subject to government investigations.

With new and developing social media platforms, government agency Facebook pages, YouTube channels, blogs and Tweeters have begun to emerge and proliferate. The General Services Administration ("GSA"), Small Business Administration ("SBA") and Office of Management and Budget ("OMB"), Health and Human Services ("HHS") and Centers for Disease Control and Prevention (CDC) have all been early pioneers of social media and micro-sites. This interaction among government and the public using social media is what is commonly referred to as "gov 2.0." Not only are agencies themselves using social media to interact, but government employees, government contractors and their employees, and companies regulated by the government and their employees are all exchanging information using social media as well.

While these new platforms provide increased accessibility and interaction, they also create significant legal risks to those that have contractual or regulatory interactions with the government.

Social Media in Action in Government Contracts & Investigations

Government Contracts

State and federal government contractors have a particularized interest in social media experience because they often obtain access to sensitive government information and systems, and as a result will be required to comply with forthcoming government regulation of social media. Risks to information and system security, to privacy, and other risks associated with the use of social media prompted the Federal Chief Information Officer ("CIO") Council to issue Proposed Guidelines on the Use of Social Media by Federal Departments and Agencies in September 2009. The CIO's proposed guidelines note pervasive risks associated with social media, suggest that each agency must make individual cost benefit calculations prior to creating an agency social media interaction, and recommend a series of both non-technical/policy and technical security controls to protect government information and security.

Once government policies are finalized and adopted, government contractors will be required to navigate interaction with the government using new social media interface, and maintain compliance with proposed limits or face risks associated with non-compliance. In particular, contractors who have access to sensitive and classified information or information systems will be required to establish robust compliance programs in place to security. Contractors who fail to address these issues may be at a disadvantage to companies who do or may be prevented from obtaining government contracts. Moreover, contractors without compliance programs subject themselves to the same privacy, security, and other risks associated with social media that concern the government.

Furthermore, as a result of gov 2.0, government information and communications are happening faster and being shared with a wider audience. Government contractors can develop strategies consistent with applicable law to take advantage of gov 2.0 and use social media as a tool to their competitive advantage.

Government Investigations

In the course of state and federal government investigations, companies that are regulated by the government or subject to civil or criminal investigations are often confronted with information derived from social media sources, or asked to produce or provide information in regard to social media. These companies must understand the breadth of regulation of social media and set appropriate operating procedures pertaining to records management and document retention. Companies also should set the terms and conditions on social media use for their employees to ensure that information flow is appropriately managed, and to prevent unwarranted disclosures before, during, and after government investigations.

Bottom Line—What You Need to Do

Contractors, companies in regulated industries, and those subject to government investigations cannot ignore the significant risks, forthcoming regulations, and new interactive opportunities associated with the proliferation of social media. These entities should develop a social media operating and compliance program and comprehensive strategy to mitigate risks, protect information and information systems, and streamline interface with government social media programs.

— CHAPTER 6 —

Insurance Recovery

Chapter Author

Carolyn H. Rosenberg, Partner – crosenberg@reedsmith.com [143]

Introduction

This chapter looks at the relationship between social media and insurance in two respects: first, when buying or renewing insurance, what types of policies or enhancements should be considered; and second, if a claim or potential claim arises, what should you or your company do to maximize potential insurance recovery.

Social Media in Action in Insurance

Considerations When Purchasing Insurance

Social media claims or potential claims may arise in almost any context, from branding and advertising issues to defamation and privacy claims, to consumer class actions and securities claims.[144] As a result, when considering purchasing or renewing insurance coverage, the steps outlined below may be helpful.

Inventory Current Policies That May Provide Coverage

Companies traditionally carry directors' and officers' ("D&O") liability, professional liability ("E&O"), comprehensive general liability ("CGL"), property damage and "business interruption" coverage, fidelity bond policies and fiduciary liability policies. They may also have employment practices liability ("EPL"), cyberliability and, most recently, data privacy and security liability specialty coverages. Since claims may raise a variety of issues and take different guises—from common law fraud and misrepresentation claims to invasion of privacy and cyber extortion—looking at an inventory of policies with a "social media" lens can assist in seeing and seeking potential coverage that may come into play. One thing is certain: cybercrimes will continue to grow.[145]

For example, a CGL policy typically provides coverage for bodily injury and property damage, as well as for advertising and personal injury claims. But the language should be examined to determine if there are terms, conditions or exclusions that limit or expand coverage. For example, some definitions of "property damage" may exclude electronic data, while a coverage endorsement may specifically provide some coverage. "Personal Injury" typically includes publication or utterances that are in violation of an individual's right to privacy, defamatory or disparaging. Although whether and how these coverages may apply depends on the provision, facts and applicable law, insurance-policy wording should be negotiated when analyzing the potential "buckets" for coverage should a claim be made. Similarly, a defamation claim may become an employment-related claim and coverage under an EPL policy should be examined to see if there are any obvious exclusions or subtle restrictions that can be addressed when negotiating the coverage. Being pro-active in negotiating coverage before a claim arises affords much greater leverage if and when the claim hits.

Consider New Products and Recognize They are Also Negotiable

Several years ago, cyberliability and Internet-related liability policies were introduced to the market. The first versions were difficult to assess given that claims were still emerging and the policies were not yet tested. The early specialty policies also contained exclusions that threatened to engulf the coverage provided. As more insurers have entered the market, claims have matured, and underwriters have become more comfortable with underwriting the risks, and the policies have improved. Policyholders who are willing to invest in reviewing and comparing choices and wording can tailor the coverage to their needs and potential exposures. For example, some technology, media, data privacy breach and professional liability policies provide coverage for first-party loss (damage suffered directly by the company), including internal hacker attacks or business

interruption, or expenses to maintain or resurrect data. Coverage for third-party loss (claims asserted against the company by third parties), is also available.

Coverage for third-party loss may include reimbursement of defense costs and indemnification for judgments and settlements. The claims may include allegations of violations of privacy rights, and personal information, duties to secure confidential personal information under state and federal laws and regulations, breaches by employees or others, infringement of intellectual property rights, unfair competition, defamation and consumer protection, and deceptive trade practices statutes.

The coverage may include regulatory actions, lawsuits, and demands. Coverage may also apply to "breachless" claims where a potential problem or disclosure can be fixed before it becomes a claim.

Key Coverage Enhancements to Seek

A Broad Definition of Claim. Coverage should apply to demands, investigations and requests to toll a statute of limitations, as well as to complaints, civil, criminal, and administrative and regulatory proceedings. Keep in mind that a broader definition of Claim also means a corresponding obligation to report what will now be a Claim.

A Broad Definition of Loss. Loss should encompass a broad array of relief, including statutory fines and penalties where insurable, as well as defense and investigative costs.

Narrowed Exclusions. Exclusions should be narrowly tailored and contain "exceptions" where coverage will be provided. Defense costs should be covered, and the exclusions should be severable, so that one "bad apple" doesn't spoil coverage for others.

Defense and Settlement Flexibility. Consider whether the insurer provides a defense or the insured seeks control over the defense. Negotiate "consent to settle" provisions.

Seek Coverage Grants via Endorsement. Specialty or tailored endorsements may add coverage and should be requested.

Maximizing Potential Coverage When a Claim Arises

Maximize the Potential for Insurance Recovery

Insurance may provide valuable protection for current loss, as well as for potential and actual claims. To maximize recovery:

Gather All Potentially Relevant Insurance Policies or Indemnity Agreements. As discussed above, key policies may include commercial crime or fidelity bond policies for internal theft; data privacy and security or cyber coverage for claims as a result of potential breaches of security and access to private data; CGL and property policies for potential business interruption claims; D&O coverage for potential breaches of fiduciary duty against directors and officers or securities claims based on alleged stockdrop or financial disclosure issues. Any indemnification agreements with vendors or other third parties who may owe contractual obligations to the company should also be reviewed, as well as any insurance policies where the company may be an Additional Insured.

Provide Timely Notice of Breaches, Claims or Potential Claims to All Primary and Excess Insurers. Insurance policies include provisions for reporting potential breaches, claims, occurrences or loss, and should be adhered to carefully. Failure to comply may result in a coverage dispute or denial of coverage, depending on the policy requirements and applicable case law. Provisions differ by policy. For example, a fidelity bond policy will specify when the initial notice is to be provided, and a proof of loss must be filed within a designated time period of reporting the initial loss. D&O policies allow reporting of potential, as well as actual claims. If the claim develops, it is "parked" in the policy in which the initial notice was provided. Claims and potential claims should be reported to both primary and excess carriers across all programs to avoid later challenges of "late notice."

Obtain Consent to Defense Arrangements. Some insurance policies have a "duty to defend," meaning that the insurer must provide a legal defense for insureds under the policy. Other types of policies provide for "reimbursement," where the insured assumes its own defense obligations, subject to the insurer's advancement or reimbursement of defense expenses. The insured typically is required to obtain the insurer's consent to defense arrangements, which may not be unreasonably withheld. Communication with insurers at the earliest stage of a claim is important to address defense arrangements. For example, if policies with both "duty to defend" and

"reimbursement" obligations apply, the insured can assess how best to manage the defense arrangements. Similarly, if the insurer proposes specific counsel but the insured objects, depending on the coverage defenses raised by the insurer and applicable law, the insurer may be obligated to pay the cost of "independent" counsel for the insured, or the insured may have to retain and pay for separate counsel to monitor the defense.

Adhere to Cooperation Obligations and Respond to Requests for Information and Coverage Defenses. Although the language of insurance policies differs, an insured generally has an obligation to cooperate with all reasonable requests of insurers. Insurers also typically have a right to associate—that is, to consult with defense counsel or, in some cases, participate—in the defense and settlement of claims involving or potentially involving their coverage.

These responsibilities of the insured may differ depending on the type of policy and whether the insurer is defending the claim. Insureds should recognize, however, that the policy language, relevant case law and individual, specific circumstances will dictate what is required or reasonable in a given context. For example, insureds typically do not have an attorney-client privileged relationship with an insurer, especially in a non-duty to defend situation. Consequently, an insured would need to be very careful in sharing information with insurers. Confidentiality or joint defense agreements may provide some protection of sensitive disclosures, but knowledgeable counsel should be consulted to provide guidance. Insurers may also seek to interview witnesses, employ investigators, and seek out defense counsel's analysis or fee statements. Again, these requests must be carefully examined with an eye toward insurance coverage and privilege considerations.

Insureds should also promptly respond to letters or other communications raising coverage defenses or denying coverage. Potential exclusions or other terms and conditions may not apply or may limit coverage only for part of a claim. Even if it is too early in the process to discern the full extent of coverage, an insured should make a record disagreeing with the carrier's restrictive coverage positions, and reserve its right to supplement its response. Moreover, a strong letter replying to coverage-challenges may result in a reversal of a coverage denial. Obtaining the positions of the insurer(s), especially early in the process, may also help expedite a coverage determination through litigation, mediation or arbitration if informal negotiation is unsuccessful.

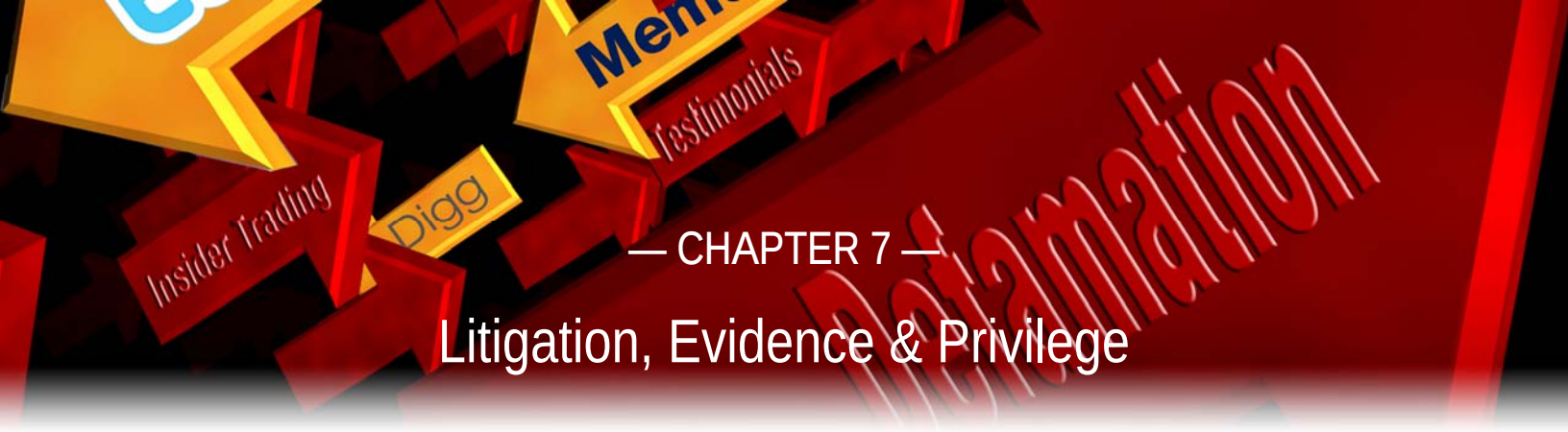
Obtain Consent to Settlement or Payment of Judgment. Know your rights and obligations. Insureds should check for any "hammer" provisions, which may limit the insured's recovery if the insured refuses to settle where the insurer is able to resolve the underlying claim. Conversely, where the insured desires to settle but the insurer does not readily agree to pay the claim, the insured should review the "consent" provisions of the policy. Typically, consent to a settlement cannot be unreasonably withheld, but policies may also specify that the insurer has a right to participate in the negotiation of a settlement or that an "offer" to settle requires insurer consent. Managing the insurer-insured relationship throughout the claim process in a thoughtful and diligent way will typically put the insurer and insured in a better position to reach agreement, than if the insurer is not promptly brought "into the loop."

Resolve Coverage Disputes. If informal negotiation does not resolve a dispute, the policy may dictate the next steps to follow. Policies may contain provisions requiring that an insurance dispute be mediated, arbitrated or litigated in a particular jurisdiction, or that a certain state or country's law be applied to the coverage dispute. These provisions should be identified early in a dispute so that strategy can be considered. Moreover, excess policies may include a different provision for resolving disputes than does the primary coverage policy(ies), making resolution of a major claim potentially challenging. Knowing the applicable rules early on will make navigating the settlement course easier.

Consider Lessons Learned for Renewal. Terms, conditions, exclusions or other difficulties in resolving claims may be considered in negotiating coverage with the same or other insurers for the next year. In addition, insurance applications may request information about current pending and/or potential claims. Such applications or requests for information should be reviewed with counsel, as applications and attachments may be disclosed in litigation discovery. Worse, they may become the basis for potential actions by insurers to rescind or void the policy.

Bottom Line—What You Need to Do

As social media claims continue to develop, so, too, will insurance policies. During this fluid process, companies can best arm themselves with good risk management, comprehensive coverage, and sensitivity to managing and maximizing their relationships with insurers.



— CHAPTER 7 —

Litigation, Evidence & Privilege

Chapter Authors

Alexander "Sandy" Y. Thomas, Partner – athomas@reedsmith.com

Maureen C. Cain, Associate – mcain@reedsmith.com

Introduction

This chapter looks at the relationship between social media and litigation practices.

Millions of employers, employees, and jurors use social media such as LinkedIn, company websites, Facebook, Twitter, MySpace, and YouTube for business and personal reasons. Users of social media are often very candid and tend to post messages and photos with little thought in an informal, spur-of-the-moment manner from smart phones, blackberries, and personal computers. Social media postings often include details that the user would never disclose directly in a formal correspondence, and certainly not to the boss of their company or to an opposing attorney if litigation were involved. Moreover, many people using social media do not realize that such postings often become a permanent record, even if the items are removed.[146]

Lawyers have begun researching social networking sites to gain information about all aspects of a case, including the parties on the other side, how a particular business is conducted, the witnesses, and the jurors. Social media sites contain valuable information such as messages, status updates, photos, and times of every posting, all of which can be used to undermine an opponent's case in litigation, and can even negatively affect a company's business and public image.

This chapter describes various real-life examples of how social media has been used to undermine an opponent's case in litigation and to negatively affect the image and business of various individuals or entities. Specifically, this chapter discusses how social media has been used to impeach witnesses, uncover documents that would ordinarily be protected by the work product or attorney client privilege, and expose juror misconduct. As an employer, it is important to understand and educate all employees and in-house counsel on the risks associated with social media, how it can undermine the company's legal positions, and ultimately its effect on business operations and public relations. (*See Chapter 4 Employment*.)

Social Media in Action in Litigation

The Use of Social Media to Impeach Witnesses

Social media sites may contain contradictory statements, character evidence, or other evidence that can be used to impeach witnesses during litigation. Below are a few illustrations:

- In July 2008, Trisha Walsh Smith made a YouTube video regarding her bitter divorce from Broadway mogul Phillip Smith. In the video, Ms. Smith complained about the terms of her prenuptial agreement and made embarrassing sexually based remarks about her then-husband. After reviewing the post, the judge presiding over the case refused to change the terms of the prenuptial agreement and granted the husband a divorce on the grounds of cruel and inhumane treatment.[147]
- In *People v. Liceaga*, 2009 WL 186229 (Mich. App. 2009), the defendant was convicted of second degree murder and possession of a firearm during the commission of a felony after shooting a friend in the head. The defendant admitted to shooting his friend, but claimed it was an accident. The principal issue at trial was defendant's state of mind at the time of the shooting. Pursuant to Michigan Rule of Evidence

404(b)(1) involving prior act evidence, the trial court allowed the prosecution to introduce a picture of defendant from his MySpace.com website that depicted him holding the gun that was used to shoot his friend and displaying a gang sign with his hands. After defendant was convicted, he appealed, arguing that the MySpace photograph was inadmissible. The Michigan Court of Appeals affirmed the trial court's evidentiary ruling, stating that three witnesses used the photo to identify the defendant as the person who previously threatened them with the gun used in the case, and it was relevant for showing the defendant's familiarity with the weapon used in the offense.

- Shortly after severely injuring a young woman while driving under the influence, Joshua Lipton posted a photo of himself on Facebook jokingly wearing an orange prison jumpsuit during a Halloween party. The Rhode Island assistant attorney general displayed the photo in court as part of a PowerPoint presentation with the title "Remorseful?" over the photo. The judge presiding over the case focused in part on the photo when deciding to sentence Lipton to two years in state prison for his DUI.[148]

As the above examples illustrate, users of social media often fail to consider the consequences of their posted statements and photos prior to such postings. In the corporate world, analogous postings could be made by employees regarding a wide range of work-related issues, including comments concerning layoffs that implicate the Age Discrimination and Employment Act, disclosures of intellectual property and trade secrets in various career-oriented chat rooms or blogs, and gossip about a sexual harassment or white collar crime internal investigation. It is imperative that a company's managers, supervisors, and employees are educated on the implications and discoverability of such postings so that their use of social media does not undermine legal positions in a future or pending lawsuit against the company. (*See Chapter 4 Employment*.)

The Waiver of the Work Product Doctrine and Attorney Client Privilege Through Social Media

The use of company websites and other social media also provide real opportunity for waiver of the work product doctrine protection and attorney client privilege through public disclosure of confidential information. Below are a few examples:

- In *Kintera, Inc. v. Convio, Inc.,* 219 F.R.D. 503 (S.D. Cal. 2003), Kintera sued its competitor Convio for copyright infringement and misappropriation of trade secrets after Convio allegedly obtained a CD Rom belonging to Kintera containing proprietary and confidential computer program codes relevant to both companies' Internet-based marketing and fundraising services. For commercial reasons, Kintera discussed the alleged misappropriation of trade secrets on its company website, and noted that it had obtained signed affidavits under penalty of perjury from Convio employees. During discovery, Kintera tried to withhold the affidavits from Convio pursuant to the work product doctrine but, based on the disclosures of the affidavits on Kintera's website, the court rejected Kintera's objections and ordered that Kintera produce the witness statements contained in the affidavits.

- In *Stern v. O'Quinn*, 253 F.R.D. 663 (S.D. Fla. 2008), Howard K. Stern, the attorney and companion of Anna Nicole Smith, filed a defamation action against John M. O'Quinn & Associates after the firm allegedly made defamatory statements about Mr. Stern to the media while representing Ms. Smith's mother, Virgie Arthur. Around the same time, a book was published entitled *Blond Ambition: The Untold Story Behind Anna Nicole Smith's Death*, which accused Mr. Stern of numerous criminal acts. An investigator for the book, Wilma Vicedomine, discussed the results of her investigation with the author and also made numerous statements in on-line chat rooms regarding her investigative progress including strategy, efforts to have Mr. Stern prosecuted, and conversations she had with Ms. Arthur. During discovery, plaintiff sought documents from the O'Quinn law firm that supported the statements made by the firm to the media. Furthermore, the discovery requests sought to determine the firm's efforts in investigating whether the statements it made about Plaintiff were true or false, including the statements made by Ms. Vicedomine for the *Blond Ambition* book. The firm tried to argue that the investigation for the book was protected by the work product doctrine but the court rejected such an argument because, *inter alia*, the contents of the investigation were published in chat rooms and to the author of the book. Accordingly, the court required the production of all postings in the chat rooms and all documents and statements provided to the author of the book.

As the above-examples demonstrate, users of social media must be careful when disclosing personal or business information on-line in order to ultimately protect themselves from waiving the work product doctrine or attorney client privilege in future or pending litigation. It is often sound

business strategy for a company to post statements on its website to keep the public informed on various issues and ensure public confidence in the company's product and services, bolster public relations, and increase profitability. However, if a company discloses too much, there are instances where it will risk waiving work product and attorney client communication protections. Managers, supervisors, or employees who disclose work-related issues in chat rooms and blogs run the risk of waiving both privileges as well, forcing a company to produce documents they ordinarily would have every right to withhold in litigation. Thus, it is essential that all managers, supervisors, and employees understand the implications of discussing work-related issues on-line and to realize that certain postings will come back to haunt the employees and the company for which they work.

Social Media Use by Jurors

Social media can have a particularly pernicious effect on jury trials. In several recent instances, jurors have made inappropriate disclosures concerning corporate and individual litigants during the pendency of a trial. Businesses should police social media postings while a trial is ongoing to protect themselves from the consequences of such postings. Below are a few examples where such posting have been made:

- In March 2009, Stoam Holdings, a building products company being sued for allegedly defrauding two investors, asked an Arkansas court to overturn a $12.6 million judgment, claiming that a juror used Twitter to send updates during the civil trial. The juror, Jonathan Powell, sent Twitter messages including, "oh and nobody buy Stoam. Its bad mojo and they'll probably cease to Exist, now that their wallet is 12m lighter" and "So Jonathan, what did you do today? Oh nothing really, I just gave away TWELVE MILLION DOLLARS of somebody else's money." The trial court denied the motion seeking to overturn the verdict and the attorneys are currently appealing.[149]

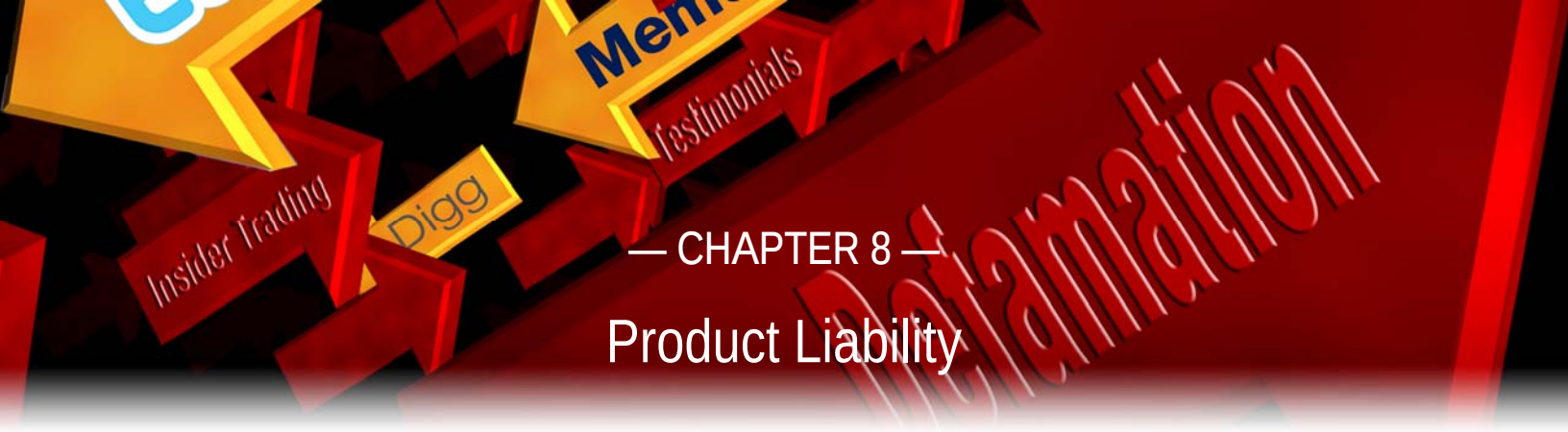
- In August 2009, two jurors in a murder trial had posted Facebook comments critical of jury duty and the length of trial. One Facebook Friend responded by stating, "Fry him." A second responded that the juror should "Just vote guilty and get it over with."[150]

- In March 2009, defense attorneys in a federal corruption trial of a former Pennsylvania state senator, Vince Fumo, demanded before the verdict that the judge declare a mistrial because a juror posted updates on the case on Twitter and Facebook. The juror even told his readers that a "big announcement" was coming on Monday, prior to the verdict. Judge Buckwalter decided to let the deliberations continue, and the jury found Fumo guilty of all 137 counts charged in the indictment. His lawyers plan to use the Internet posting as grounds for appeal.[151]

As the above examples indicate, the use of social media by jurors during a trial may impact a company's public image, business, and stock price if a juror leaks information about his or her perception of the case prior to the final verdict being rendered by all jurors. The use of social media by a juror may be grounds for a mistrial or an appeal because the social media postings of the juror may indicate that the juror was biased and was making a decision prior to reviewing and considering all evidence. Retrying a case and/or taking an appeal are both time-consuming and costly for companies. To prevent the above injuries to a company, it is essential that explicit instructions are given to the jury prior to the commencement of trial prohibiting the use of social media. Furthermore, it is wise for companies and their legal team to research the social media sites during the trial to ensure that no juror is leaking the jurors' thought process about the case to the public and/or being tainted by other individual's responses to any postings on the social media sites.

Bottom Line—What You Need to Do

What is said on social media sites can and will be used against you and the company for which you work in a court of law, the court of public opinion, and ultimately the business world. Accordingly, it is essential that all managers, supervisors, employees, and in-house counsel be educated on the pitfalls involved with social media to prevent such postings from undermining your company's legal position, business relations, and public image.



— CHAPTER 8 —

Product Liability

Chapter Authors

Antony B. Klapper, Partner – aklapper@reedsmith.com

Jesse J. Ash, Associate – jash@reedsmith.com

Introduction

This chapter examines the relationship between social media and product liability.

Companies that develop products, such as pharmaceutical and medical device companies, utilize social media in a variety of ways, including internal and external blogs, pages on third-party sites such as Facebook, and other third-party sites that provide reviews concerning the use and safety of a company's products. These social media sites and platforms can lead to a wealth of positives for companies. More readily available information can mean greater knowledge about the products and therefore greater sales. However, this same informational accessibility may also create problems. Companies that develop products are always at risk for lawsuits related to the safety profile of those products, and the use of social media can lead to (1) new legal claims and increased exposure to punitive damages, as well as (2) weakened defenses to claims not based directly on social media.

Social Media in Action in Product Liability

New Claims and Increased Exposure

The pharmaceutical and medical device industries are heavily regulated. Specific rules govern what information a company can relay to patients or doctors through warning labels, package inserts, written correspondence, or visits to a doctor's office by a company's sales department.[152] Any communication by a company outside these regulatory parameters may be used against the company as evidence that the company acted in violation of government regulations, leading to a host of potential causes of action under strict liability and negligence theories.[153] For example, if a company has a blog or chat room where patients and/or doctors correspond with the company, this direct communication may include off-the-cuff comments that contains language outside the parameters of information the company is allowed to relay regarding its products.[154]

Although these problems can occur even without social media, the sheer magnitude of social media outlets and the relative informality of their content greatly increases the risk that statements will be made that may be actionable in a court of law. Similarly, social media exchanges leave a virtual paper trail that can be reviewed for an improper communication in a way that oral communications between a sales representative and a doctor, for instance, cannot.

A common cause of action stemming from such improvident statements or omissions is the consumer fraud claim. Consumer fraud claims are usually easier to prosecute than traditional negligence or other product liability claims because in many jurisdictions, the elements of proof usually do not require proof of causation or reliance. Not surprisingly, the bread and butter of an effective plaintiff lawyer's practice is finding and marshaling those company statements that allow them to pursue these types of causes of action. If successful (because a company has been less than circumspect in what it says), these plaintiff lawyers not only have a better chance of pursuing their underlying claims, but they are also better positioned to secure large damage awards, including punitive damages.

An effective plaintiff lawyer is always looking for documents that show a company "puffing" or over-extolling the efficacy and safety of its products. Better yet are those documents that show a company making efficacy and safety claims

about its products that are perceived as not entirely consistent with the company's "confidential," internal documents. When these inconsistencies arise—particularly when a company's marketing department is not working closely enough with legal and risk management—the plaintiffs are not only well-positioned to advance their underlying claims, but they are also able to demonize the company as putting profits over safety or simply as lying to its customers.

Additional problems can arise when a company sponsors third-party websites to promote its products. If the company has editorial rights over the content of the site, plaintiff attorneys may be able to convince a jury that a company "ghost writes" information. "Ghost writing" articles or promotion materials takes place where a company pays an author to write an article that helps the company sell more product—*i.e.*, the article states that a product does not cause an adverse event or that a product helps to solve a medical issue. Even if the research is sound, articles "paid for" by a company tend to look underhanded and less than sound in the eyes of the public. Where a company sponsors a site and has the ability to change content, plaintiff most certainly will conjure a "ghost writing" argument if litigation ensues with the effect of having the jury believe the company did not have the public's best interest in mind. Similarly, using editorial rights to silence views critical of the company's products—or favoring a competitor—would provide further grounds for a plaintiff lawyer. In addition, "ghost writing" can lead to unwanted, negative media attention for any entity that is accused of using ghostwritten material for its benefit.[155]

If successful at portraying a company as a bad corporate actor, the plaintiff attorney inevitably has an easier time proving all elements of plaintiff's claims (liability and causation) and positioning herself to secure a punitive damages award.

Weakened Defenses

In addition to increasing a company's exposure to legal claims, messages in social media directed to consumers, patients and/or doctors may also impact a company's defenses. For pharmaceutical companies, the learned intermediary defense greatly helps manufacturers in product liability litigation where the claims are based on a strict liability or negligent failure-to-warn claim. A vast majority of states have adopted the learned intermediary doctrine, whereby a manufacturer of a product is only responsible for adequately warning a physician, *not* the patient, about the risks of a particular product.[156] A plaintiff must prove that the prescribing physician received an inadequate warning, and if the physician had received an adequate warning, the physician would not have prescribed the product to the patient-plaintiff. In many cases, these are hard issues for a plaintiff to prove, as what the prescriber did and thought (not what the patient did and thought) becomes paramount. Social media has the potential to erode this important defense.

Any evidence that the company directly corresponded with a plaintiff (through blogs, chat rooms, or third-party sites) about information related to the language in the company's warning materials—*i.e.*, warning labels, package inserts—might convince a court that the learned intermediary doctrine does not apply since the company's words may take the place of the language of the warning label and any information provided to the prescribing physician. The loss of the learned intermediary defense would be a huge blow to any defendant-company litigating a failure-to-warn claim, allowing a plaintiff to offer self-serving testimony about the lack of sufficient warnings and instructions and their impact on plaintiff, if given.

Current Legal and Regulatory Framework

FDA regulations include rules on labeling, and written and oral communications with doctors and patients. While the FDA regulations do not contain guidance specifically on the use of social media, a November 12-13, 2009, Public Hearing likely will lead to rules on its use in 2010.

Bottom Line—What You Need to Do

By its very nature, social media often begets informal dialogue that is broadcasted more widely than traditional marketing media. The more that is said publicly, the greater the risk that what is said does not square with regulatory requirements, and with what is said privately in internal, confidential company documents. For this reason, a company that chooses to use social media as a marketing or information tool must involve legal and risk management departments in reviewing marketing's use of chat rooms, blogs, and external third-party websites (and the content in those media). The failure to do so can result in heightened exposure to legal claims, large damages, and weakened defenses.

Bottom Line—What You Need to Do

Social media implications and applications to advertising and marketing cannot be ignored. That is where the consumers are, and where consumers go, marketing dollars ultimately follow. All companies, regardless of whether or not they elect to actively participate in the social media arena, should have policies in place to determine how to respond to negative comments made about the company and/or its brands. Companies that seek to play a more active role should have policies in place that govern marketing agency and/or employee interaction with social media, as well as the screening of UGC. It is critical, however, that companies not simply adopt someone else's form. Each social media policy should be considered carefully and should address the goals and strategic initiatives of the company, as well as take into account industry and business specific considerations.

— CHAPTER 9 —

Securities

Chapter Authors

Christopher P. Bennett, Partner – cbennett@reedsmith.com

Amy J. Greer, Partner – agreer@reedsmith.com

Jacob Thride, Associate – jthride@reedsmith.com

Introduction

This chapter looks at the relationship between social media and the Securities sector. Securities issuers, investors and other participants in the securities markets, as well as regulators, have always been quick to embrace new technology and forms of communication—social media is simply the newest iteration. For example, major financial institutions have numerous Facebook pages and even the U.S. Securities & Exchange Commission ("SEC") now has a Twitter feed.

We begin by examining the use of social media by issuers to disseminate information to the public. In addition, we consider how companies can use social media for advertising or promotion. Next, we look at potential liability that may arise when issuers, their employees, or business partners share information via social media. Finally, we examine how companies can be victimized when social media is exploited to manipulate the market in a company's stock, or to disclose misappropriated (or stolen) material non-public information (*e.g.*, false rumor cases, market manipulation).

Social Media in Action in the Securities Sector

Making Information Public

Recognizing that the availability of the Internet has broadened substantially, and that, for example, more than 80 percent of mutual fund share owners have Internet access, Regulators have taken steps to permit (and even encourage) disclosures and other communication electronically.

Moreover, in addition to encouraging the use of electronic disclosures, the SEC has focused on improving the character of those disclosures by promoting disclosures containing interactive data. Interactive data refers to financial data, or other disclosure information, that has been tagged using XBRL (eXtensible Business Reporting Language) or another method. XBRL is an electronic markup language that is used to communicate financial and business data electronically by allowing the individual elements of a financial statement to be electronically tagged. XBRL tagging allows the user to separately manipulate and analyze the elements of a financial statement, for example, including footnotes and financial statement schedules, for interactive comparisons and calculations. In June 2009, the SEC adopted final rules, which will be phased in over a three-year period, requiring public companies to provide financial statement information using XBLR.

Regulation FD governs the public disclosure of material information and requires that such information be disseminated by methods of disclosure "reasonably designed to provide broad, non-exclusionary distribution of the information to the public." The SEC has been moving toward recognizing more channels of distribution for required and other public information disclosures (either to meet regulatory obligations or in connection with individual securities transactions), including a variety of electronic media, and the SEC has acknowledged that as technologies expand, it will continue to recognize new channels of distribution as appropriate for such disclosures. In time, social media may become one of these recognized channels. In the short term, however, it is likely that social media, coupled with traditional forms of shareholder

communication, could provide companies with the ability to more effectively reach more actual or potential customers, investors and/or shareholders. While social media presents an attractive channel of communication, care must be taken to assure that disclosures are appropriate and conform to a variety of applicable legal standards, and that those standards are understood and adhered to by a company's employees and agents.

Failure to comply with Regulation FD could well result in an enforcement investigation or action. In addition, noncompliance with Regulation FD makes a company vulnerable to an SEC investigation or proceedings relating to trading violations if the recipients of information disclosed by the company in a discriminatory manner trade their shares ahead of a more fulsome public disclosure.

While application of the securities disclosure framework to social media continues to develop, issuers should be familiar with the current guidelines released by the SEC August 7, 2008, and subsequent compliance and disclosure interpretations issued August 14, 2009, relating to the use of company websites for such disclosures. These guidelines begin to outline boundaries applicable to sharing information through social media outlets, as well as the potential for issuer liability for information they or their employees post on blogs, networks, communities and discussion forums. While it appears that issuers can utilize social media to disseminate information to the public, they need to proactively analyze the SEC guidelines and establish internal policies and frameworks to address these issues.

Advertising and Promotion

Social media also offers an opportunity to provide information in connection with a transaction, to promote a particular investment or investment strategy and, as such, could be a very effective and attractive tool for investment advisors, investment companies and broker-dealers. However, if the promotion or disclosure is held to be inadequate or otherwise violative of regulatory requirements, it could result in an investigation or action by regulatory authorities. For example, numerous registered investment advisors ("RIAs") use social media platforms such as Facebook, MySpace, LinkedIn, YouTube, Twitter and blogs for business purposes because social media is an inexpensive and effective way for them to communicate with clients and prospective clients.

Investment advisers, investment companies, broker-dealers and other regulated persons and entities must take great care to assure that they obtain the proper approval before using social media tools. For registered representatives ("RR") subject to the Financial Industry Regulatory Authority ("FINRA") regulations, this means obtaining the approval from their broker-dealer compliance department before posting anything on the Internet. Postings are considered advertisements, and FINRA has published guidelines for use of the Internet by registered representatives of broker-dealers.

The SEC has similar guidelines that RIAs must adhere to that govern advertisements, including postings to public Internet forums[157]. RIAs are generally responsible for self-supervision by chief compliance officers. In light of the foregoing, it seems RIAs not subject to FINRA regulations have quite a bit more flexibility when using the Internet and social media. However, common sense should always be used to avoid publishing security recommendations or any testimonial, both of which are explicitly prohibited by the SEC and state regulatory authorities. Even though communications with current clients are not usually viewed as advertisements, they might fall into that category if circumstances suggest that their purpose is to sell additional advisory services or to attract new clients. If an RIA's use of social media is viewed by the SEC as an advertisement, it is subject to Rule 206(4)-1 under the Investment Advisers Act of 1940.

Certain types of social media, expressly or implicitly, violate Rule 206(4)-1(a)(1)'s prohibition of testimonials. A testimonial is a statement relating to a client's experience with, or endorsement of, an RIA. LinkedIn profiles, for example, allow RIAs to accept and to publish professional recommendations from other individuals using the business-oriented social networking site. Any published recommendation that references the RIA may be construed as a testimonial, regardless of whether it was solicited, and it might violate Rule 206(4)-1 even if the person making the recommendation is not a client. These recommendations might be viewed as false or misleading, since an RIA may have solicited them from a friend, relative, or business associate. Regulators may see these recommendations as some sort of quid pro quo (*e.g.*, an RIA recommends someone and that person returns the favor). These recommendations also may paint a misleading picture of the RIA, since negative comments are unlikely to be published on the RIA's profile.

In light of the foregoing, these recommendations might violate Rule 206(4)-1(a)(5), which bars any advertisement that is false or misleading in any way. Twitter and Facebook raise similar compliance issues.

Even if social media content is not considered to be a testimonial, a Tweet or other communication can still violate Rule 206(4)-1. RIAs may send messages in haste, thereby increasing the risk of sending false or misleading information. Also, a Tweet is limited to 140 characters, which leads to users increasingly using abbreviations in turn raising the risk that the message could be misleading or difficult to understand. Finally, the space limitations of Tweets may omit important information, including disclosures.

Profiles on LinkedIn, Facebook, and other social media platforms should be scrutinized to ensure they are not false or misleading, and should be consistent with the RIA's advisory contract, and other advertisements, including websites. All references to performance may be subject to the guidance in the Clover Capital no-action letter. The Clover Capital no-action letter requires that performance results be presented on a net-of-fees basis, and that advisers make numerous disclosures when providing performance results. In addition, RIAs may inadvertently be violating Rule 206(4)-1(a)(2) under the Investment Advisers Act, which restricts advertisements referring to specific recommendations made by an RIA that were or would have been profitable to any person.

RIAs should revise their compliance manual to incorporate policies and procedures regarding the use of social media by their employees. RIAs have three options: (1) allow employees to post information about the advisory firm but require pre-approval by a firm's compliance officer or a designee for all such business-related postings using social media (a supervisory nightmare); (2) a limited prohibition against allowing any information to be posted to the public profile portion of any social media; or (3) an absolute prohibition against employees communicating any information about the advisory firm (other than the name of their employer) on a social media site.

RIAs should make all employees aware that posting any information about their advisory firm on a social media site is considered advertising and, as such, is subject to SEC prohibitions and firm policies and procedures. An advisory firm should also require that all employees attest to the fact that they are in compliance with the firm's rules regarding advertising and electronic communications. The firm's chief compliance officer should also periodically visit the more common social media sites to check for violations of either Rule 206(4)-1 or the firm's own policies and procedures.

The fact that the SEC is now on Twitter should be of additional concern. One of the SEC's very first Tweets discussed a recent enforcement action against an RIA. It stands to reason that if the SEC is on Twitter, then it certainly is capable of finding compliance violations in social media.

Insider Trading

Social Media's "stock in trade" is the communication of information. Thus, there is an obvious likelihood that some of the information that might be conveyed via social media could be material, non-public information. The transmission of such information, if it breaches a duty to the company or to the person who shared the information, may itself be a violation of the securities laws, and if you trade on such information you very likely have committed insider trading. This conduct is regulated largely through the antifraud provisions, but most often Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder.

Underscoring its recent announcements that insider trading remains a high priority, the SEC has entered into an agreement with the New York Stock Exchange's regulatory arm (NYSE Regulation, Inc.) and FINRA, to improve detection of insider trading across the equities markets by centralizing surveillance, investigation, and enforcement in these two entities. These changes, together with recent pressure brought to bear on U.S. regulators by high-profile enforcement failures, are likely to result in increased enforcement in this area. This is true because insider trading cases, specifically, are comparatively easy for regulators to identify and investigate and, in light of public pressure, regulators have a substantial interest in bringing higher numbers of cases. At the same time, we have seen an increase in insider trading investigations and prosecutions worldwide, as well as an unprecedented level of international cooperation among securities regulators to pursue violations across jurisdictions. In particular, the Financial Services Authority in the UK has put the identification and punishment of insider trading at the top of its enforcement agenda.

Thus, social media is of particular importance when considering insider trading issues because of the volume of information traffic, the fact that the traffic crosses borders, and the ability of regulators to locate the source of the information, since social media postings—like everything on the Internet—never really disappear.

Other Potential Liability—Market Manipulation, False Rumors

Wrongly used, information posted in social media can expose companies to regulatory investigations and legal

claims, and expose companies' securities to manipulation by those who would intentionally exploit the media for unlawful activity. Companies should assure that sites, pages and other outlets for discussion and dispersal of information are being properly and lawfully used.

In much the same way that companies protect their trademarks and trade dress, they should protect their company names and their information, or risk finding themselves on the receiving end of an investigative subpoena, even in circumstances where the company itself had no involvement whatsoever. The SEC has announced its intention to pursue "false rumor" cases. This is just one variety of market manipulation, and social media is the perfect place for such rumors to grow and eventually impact stock prices. Although companies will not be able to ameliorate all such activity, reporting such conduct to regulators (and to website hosts) in the first instance is just one consideration that should be discussed with counsel.

Current Legal and Regulatory Framework in the Securities Sector

Three recent cases brought by the SEC offer cautionary tales. Although none involved the use of social media, any of the conduct for which the defendants were charged—and settled with the SEC–could have been accomplished using social media.

Violation of Regulation FD

In *SEC v. Black*[158], the defendant, the designated investor relations contact of American Commercial Lines, Inc. ("ACL"), acting without authority and without informing anyone at ACL, selectively disclosed material, nonpublic information regarding ACL's second quarter 2007 earnings forecast to a limited number of analysts without simultaneously making that information available to the public, in violation of Regulation FD. Specifically, after ACL had issued a press release projecting second quarter earnings would be in line with its first quarter earnings, the defendant sent e-mail from his home to eight analysts who covered the company, advising that second quarter earnings "will likely be in the neighborhood of about a dime below that of the first quarter," thus cutting ACL's earnings guidance in half. Needless to say, the resulting analysts' reports triggered a significant drop in the company's stock price—9.7 percent on unusually heavy volume. Although this selective disclosure occurred via e-mail, it could just have easily been accomplished on the defendant's Facebook page.

The SEC determined not to bring any action against ACL because it acted appropriately, cooperating with the investigation and taking remedial steps to prevent such conduct in the future. In its release announcing the case, the SEC noted that, even prior to defendant's violative disclosure, "ACL cultivated an environment of compliance by providing training regarding the requirements of Regulation FD and by adopting policies that implemented controls to prevent violations." In addition, the SEC highlighted that the defendant had acted alone, and that ACL, on learning of the selective disclosure, immediately publicly disclosed the information by filing a Form 8-K with the SEC.

False Rumor

In *SEC v. Berliner*[159], the defendant, a trader himself, was charged with disseminating a false rumor concerning The Blackstone Group's acquisition of Alliance Data Systems Corp. ("ADS") via instant messages to other traders at brokerage firms and hedge funds. In short order, the news media picked up the story, resulting in heavy trading in ADS stock. Within 30 minutes, the defendant's false rumor caused the price of ADS stock to plummet 17 percent, causing the New York Stock Exchange to temporarily halt trading in ADS stock. Later that day, ADS issued a press release announcing that the rumor was false and by the close of the trading day, the stock price had recovered. On the day of the rumor, more than 33 million shares of ADS were traded, representing a 20-fold increase over the previous day's trading volume. Although the defendant sent the false rumor by instant message, he could have disseminated it through social media. One could easily imagine how a false rumor could spread even faster via Twitter, wreaking havoc with an issuer's stock price.

Insider Trading

Although the misappropriated disclosures in *SEC v. Gangavarapu*[160] were made during telephone calls between siblings, the facts disclosed are exactly the sort of details you could find on someone's Facebook page: "my husband is working all hours," "my husband is traveling a lot for business," "things are crazy at work for my husband," "thank goodness, after tomorrow, things will calm down for my husband at work!"

According to the SEC's complaint, the defendant misappropriated material non-public information from his sister, whose husband was an executive officer at Covansys Corporation, and purchased $1.4 million in stock based on the misappropriated material non-public

information. Covansys was in discussions with Computer Sciences Corporation ("CSC") and another company about their interest in acquiring Convansys. During that time period, the defendant often spoke with his sister by telephone and they discussed matters such as her husband's work activities and whereabouts. For example, the defendant's sister told him that her husband was in closed-door meetings, that he was working a lot and that he had traveled overseas for work. Then, after learning from her husband that the Covansys' board of directors would vote the next day on which acquisition offer to accept, she told the defendant "by tomorrow, it's a relief, it will be over." Based on these details of his brother-in-law's working life, the defendant purchased more than 54,000 shares of Covansys stock over eight days. When the public announcement came that CSC would acquire Covansys, the next day, the price of Covansys' stock rose 24 percent, resulting in trading profits for the defendant totaling more than $361,761.

Bottom Line—What You Need to Do

Before you decide to adopt social medial as a form of communication and disclosure, you must ensure that the proper controls are in place. Whether it be material disclosures, advertising, or everyday business disclosures, you must be certain that your communications meet the regulatory requirements. For material disclosures, that means compliance with Regulation FD. For advertising of transactions or services, that means assuring that you obtain the proper approval before using social media and that you are not in violation of any regulations, such as the Investment Adviser's Act. You should verify that all mandatory disclaimers regarding forward-looking statements and financial measures are included with any electronic disclosure.

The spontaneity of social media presents a number of risks. Regularly monitoring your websites and social media presence to assure that the discussion is appropriate, the dispersal of information is compliant with the securities laws, and more simply, that these vehicles are being properly and lawfully used, is a good dose of preventive medicine. In addition, routine searches for the use of your company's name and corporate logo or other image, so as to assure that false rumors or other manipulations are not occurring.

Insider trading policies, together with good training programs that animate the dry rules and place employees into the types of real-life situations where information can be inadvertently shared, and strict controls on material non-public information, are really the only ways that companies can protect themselves. Employees must understand the importance of Regulation FD's prohibitions on selective disclosure and know to keep the company's most important confidential information internal to the company. They need to know what information they can and cannot communicate electronically in order to stay within the limits of compliance. Such programs, together with meaningful and well-circulated corporate policies, will help to prevent violations in the first instance; and if a problem should arise, the fact that your company has undertaken these steps may tip the balance in your favor when the SEC is deciding whether or not to bring an enforcement action.

Finally, social media is new territory and the rules are constantly evolving. You will have to make a decision whether it is necessary to use social media at this moment for your company to stay ahead of the curve. If so, then carefully plan, execute, and periodically revisit a strategy that ensures that your use of social media is compliant with securities laws and that you are protected against its abuse.

— CHAPTER 10 —

Trademarks

Chapter Authors

Darren B. Cohen, Partner – dcohen@reedsmith.com

Meredith D. Pikser, Associate – mpikser@reedsmith.com

Introduction

This chapter looks at the relationship between social media and trademark protection.

Social media has provided individuals and businesses alike with the ability to communicate to an infinite number of people instantly. This great advantage, however, comes with great risks, not the least of which is the appropriation of one's intellectual property. The vigilance and policing of an owner's intellectual property has become of the utmost importance as communication provided via social networks is both viral and everlasting. A global infringement that once took weeks, months or years to occur will now take shape as fast as someone can hit "enter" on his or her keyboard. And, once the infringement is out there in cyberspace, there is no way of knowing if the offending material is ever truly deleted. As more and more individuals and businesses incorporate social media into the promotion of their products and services, increasing brand awareness, they are also finding that unauthorized use of their trademarks, service marks and trade names are emerging through these same channels.

First, we will examine trademark infringement occurring on social media platforms such as Twitter and Facebook, and how their respective policies deal with infringers. Next, we will examine the issue of impersonation on Facebook and Twitter. Finally, we will discus virtual worlds and the infringement occurring therein. As this chapter will outline, protecting and leveraging intellectual property through social media is an ever-increasing demand that is fraught with legal pitfalls.

Social Media in Action in Trademarks

Trademark, Service Mark and Trade Name Infringement

Twitter, Facebook, and virtual worlds, such as Second Life, to name a few, allow their members to adopt user names, personalized sub-domain names, virtual products, and avatars creating confusion as to the source. There is little resolve to prevent an individual or entity from adopting a user name or sub-domain name that incorporates another's trademark or personal name. Nor has the law caught up with issues involving the "sale" of virtual products that bear trademarks owned by another or the creation of avatars that resemble celebrities.

Twitter

Twitter, a social networking service that allows users to send and read posts of up to 140 characters in length ("tweets") grew 1,382 percent year-over-year as of February 2009, with more than 7 million visitors in that one month alone.[161] Think about the marketing opportunities; now, think about how many people could be deceived by trademark infringers and impersonators. Upon joining Twitter, members create a username, the "identity" through which their tweets are sent and received. A recurring issue is a member registering a username that is the trademark of another or a name belonging to a celebrity.

In September 2009, ONEOK, Inc. sued Twitter for trademark infringement, alleging that the company wrongfully allowed a third party to adopt the username "ONEOK," its company trademark, from which the unnamed third party tweeted information about the natural gas distributor.[162] The complaint alleged that the messages were misleading in that they were made to appear like official statements from ONEOK when, in fact, the company had no involvement in sending them. Over the course of a month, ONEOK unsuccessfully asked that

Twitter terminate or transfer the unauthorized account. After the complaint was filed, however, the parties resolved the dispute and the account has since been transferred to the company.

Twitter does have a trademark policy in place that provides the following:

> Using a company or business name, logo, or other trademark-protected materials in a manner that may mislead or confuse others or be used for financial gain may be considered trademark infringement. Accounts with clear INTENT to mislead others will be immediately suspended; even if there is no trademark infringement, attempts to mislead others are tantamount to business impersonation.[163]

And while Twitter provides such a policy, it is unclear how well developed a plan for dealing with trademark infringement is or how well it is enforced. As a result, it remains the trademark owner's obligation to be hands-on about protecting its rights. Strategy in doing do so may include developing a standard as to what you may deem objectionable use of your trademark, using the privacy protection put in place by the social network to the best of your advantage, and, if feasible, proactively adopting any username variants of the mark you are seeking to protect, a tactic proffered by Facebook as discussed below in *Section 2*.

Facebook

Facebook has more than 300 million active users, allowing its members to connect with others, upload photos, and share Internet links and videos. A January 2009 Compete.com study ranked Facebook as the most-used social network by worldwide monthly active users.[164]

Like Twitter, it, too, has found itself defending claims of trademark infringement. Facebook, likewise, has an intellectual property infringement policy; however, Facebook's enforcement of this policy has been called into question.[165] The policy provides that:

> Facebook is committed to protecting the intellectual property of third parties. On this page, rights holders will find information regarding how to report copyright and other intellectual property infringements by users posting content on our website, and answers to some frequently asked questions regarding our policies.[166]

With respect to trademark infringement, it is unclear whether pending trademark applications and/or common law rights will be sufficient to bring a claim, or if the challenger must own a federal trademark registration. Must the mark be registered in the United States or will a challenge based on a foreign registration hold water? How will Facebook handle claims by multiple parties claiming rights in the same mark? Only time will tell.[167]

In its own effort to combat trademark infringement and name-squatting, Facebook, in conjunction with its new policy of allowing users to create personalized URLs, has implemented the following procedures:

- Trademark owners were provided with a three-day window to record their registered trademarks with Facebook, rendering those names unavailable to third-party users, and allowing the trademark owners the opportunity to register for and use those names themselves at a later date.
- Usernames names cannot be changed and are non-transferable. As a result, a username cannot be sold, and, should a user terminate his/her account, the username will become permanently unavailable.
- Only a single username may be chosen for your profile and for each of the pages that you administer.
- In an effort to prevent a user from monopolizing a commercially desirable term, generic words may not be registered as a username.

Though these efforts can help to provide some comfort to trademark owners, it is infeasible to protect any and all variations in spelling of a mark or use of a mark with a generic term, *e.g.*, "cartierwatches." Furthermore, it remains uncertain whether Facebook, under its current trademark infringement policy, will only stop uses of exact marks. Moreover, will use of the mark as only a username be enough to enact the policy or must there be infringing content on the Facebook page, or even commercial content on the page?

Perhaps Facebook should adopt a model similar to that of the Uniform Domain-Name Resolution Policy ("UDRP") used to help resolve cybersquatting and other domain name disputes. The UDRP offers trademark owners the ability to acquire or cancel a domain name registration if they can prove that (1) the domain name at issue is confusingly similar to the owner's trademark; (2) the current owner of the domain name has no right or legitimate interest in the domain name; and (3) the current owner has registered and is using the domain name in bad faith. The decision as to whether the current domain name holder gets to maintain his/her registration or whether the domain name is to be transferred or cancelled is rendered by a neutral panel. Certainly providing a uniform set of rules could only serve to help trademark owners in protecting

their marks. Not only may such policy help to avoid costly litigation, but decisions can also be rendered fairly quickly.

While privacy protection policies provided by social media sites may help to alleviate some concerns, trademark owners can pursue other legal avenues should these policies fall short. As evidenced by the *ONEOK* case discussed above, filing suit for trademark infringement or unfair competition are options to protect your valuable trademark. The Lanham Act provides that one is liable for trademark infringement if he or she "use[s] in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive…"[168] Similar "use in commerce" requirements exist with respect to claims of unfair competition[169] and dilution.[170] However, the success of any such claims depends on the definition of "use in commerce." Does a defendant have to use the social media site to sell goods or services in order to avail the trademark owner a claim for relief under the Lanham Act? Unfortunately, this question has yet to be answered definitively, though application of the Lanham Act will certainly depend on the level of commercialization.

Impersonation

Social media, such as Twitter and Facebook has also encountered problems with impersonation, an issue particularly prevalent with respect to celebrities. Twitter has even adopted an impersonation policy that states:

> Impersonation is pretending to be another person or business as entertainment or in order to deceive. Non-parody impersonation is a violation of the Twitter Rules.
>
> The standard for defining parody is "would a reasonable person be aware that it's a joke?" An account may be guilty of impersonation if it confuses or misleads others—accounts with the clear INTENT to confuse or mislead will be permanently suspended.[171]

Twitter will allow a parody impersonation to exist if the following criteria are met:

> The profile information on a parody account must make it obvious that the profile is fake, or the account is subject to removal from Twitter.com. If it's not evident from viewing the profile that it is a joke, it is considered non-parody impersonation. Non-parody impersonation accounts may be permanently suspended.[172]

Nevertheless, countless celebrities have fallen victim to imposters who have acquired usernames of well-known personalities, including Britney Spears, Peyton Manning, William Shatner, the Dalai Lama, and even the Queen of England.[173] The landmark case that brought this issue to light involved St. Louis Cardinals Manager Tony La Russa, who sued Twitter for trademark infringement for allowing an impersonator to send unauthorized and offensive messages under his name.[174] Specifically, he claimed that the unauthorized user made light of the deaths of two Cardinals pitchers, and the public was duped into believing that these statements were made by La Russa. The case was settled in June 2009.

Cases like this beg the question as to how well trademark owners can rely on Twitter to shut down imposters, even in light of such matters being brought to its direct attention. In an effort to address such concerns, Twitter has created verified accounts, a currently experimental feature, which is a tool developed to help establish the authenticity of those individuals who encounter impersonation or identity confusion on a regular basis. An account that is verified indicates that Twitter has been in contact with the person or entity the account is representing and has verified that it is approved. However, the drafter of the tweets sent from the account is not necessarily confirmed. They note that only a handful of accounts have been verified to date (and this feature is not being tested with businesses), so that accounts that do not bear the "Verified Account" badge are not necessarily fake. According to Twitter's website:

> We're starting with well-known accounts that have had problems with impersonation or identity confusion. (For example, well-known artists, athletes, actors, public officials, and public agencies). We may verify more accounts in the future, but because of the cost and time required, we're only testing this feature with a small set of folks for the time being. As the test progresses we may be able to expand this test to more accounts over the next several months.[175]

While acknowledging that it will not be verifying all accounts, Twitter claims that it will try to assist you if your account is constantly competing with parody or impersonation accounts. Despite these efforts, it is clear that there is quite a long way to go before impersonation and identity confusion can be dealt with effectively.

Virtual Worlds

Virtual Worlds are another emerging area of unease. Developed through the application of user-generated content, members create avatars that exist in an online

world. Second Life, one such 3-D virtual world where users can socialize, connect and create using voice and text chat, also allows users to create virtual products for sale online, using on-line currency to complete the transaction that is purchased with real world currency.

Trademark Infringement

Too often the virtual products offered for sale on Second Life bare the trademarks of third parties without permission to do so. By way of example, Taser International, Inc. filed a trademark infringement claim against Second Life over the sale of unauthorized virtual versions of its electronic stun guns.[176] The lawsuit was later dropped, but the liability of Linden Lab, creator of Second Life, was debated in the media.[177] One question raised was why Linden Lab could not have been protected under the safe harbor provisions of the DMCA *(See Chapter 1 Advertising)* or the CDA *(See Chapter 2 Commercial Litigation)*. After all, Linden Lab does not manufacture or sell stun guns, but merely provides the platform through which these "products" are offered for sale. The reason is because trademark infringement claims, unlike copyright claims, for example, are not covered by the DMCA or the CDA. Still, if one were to follow the logic of these statutes, it would seem that the creator of the "product" bearing the unauthorized trademark should be held liable, not the party who merely provided the platform.

A further question is whether such use of another's trademark, in fact, amounts to trademark infringement. After all, these unauthorized products are not actually offered for sale in the real world, only on-line. However, several trademark owners have actively promoted the use of their products on Second Life, including International Business Machines Corp. and Xerox Inc.[178] Therefore, there is reason to believe that a stun gun bearing the Taser trademark, was, in fact, endorsed by Taser International Inc. As such, it would seem that it is in the trademark owner's best interest to police its mark to the best of its ability in order to avoid any possible confusion with respect to source or association. Further, you want to avoid a slippery slope wherein allowing wrongful use of one's intellectual property in the virtual world leads to even greater harm in the real world.

As IP practitioners know, infringement arises when there is a likelihood of consumer confusion among the relevant purchasing public. On this basis, a plaintiff suing for trademark infringement may claim damages based on lost or diverted sales, which, on its face, may not seem to clearly apply to the unauthorized use of trademarks in the virtual world. However, real profits are, in fact, generated on such sites. Moreover, as noted by the Intangible Asset Finance Society:

> it is undeniable that the virtual world population and the "real" life population overlap, and behavior in one medium can surely have an effect, adverse perhaps in this case, on the other. This type of activity may further prevent one from being able to fully exploit IP rights and build IP equity, in particular brand equity, by weakening, diluting and tarnishing trademark rights or serving as a barrier to potential licensing opportunities and avenues.[179]

Other examples of virtual world trademark infringement include two cases involving the company Eros LLC. In one instance, Eros sued Leatherwood for the making and selling of unauthorized copies of its virtual adult-themed "animated" bed, using Eros' "SexGen" mark.[180] Eros sought an injunction and Leatherwood defaulted. In another case, Eros, along with other Second Life merchants, sued a party for duplication of its products and selling them at virtual yard sales, using its marks to identify the products.[181] Eros had owned a pending application with the U.S. Patent and Trademark Office for the mark "SexGen" (which has since matured to registration)[182], and a second plaintiff, DE Designs, owned a federal registration for the mark "DE Designs."[183] The plaintiffs were granted a judgment by consent, wherein it was ordered that the defendant:

- pay plaintiffs $524 as restitution for profits derived from the unauthorized copying and distribution of the plaintiffs products
- represent to the court under penalty of perjury that any remaining unauthorized copies were destroyed
- permanently cease copying, displaying, distributing or selling any of the plaintiffs' merchandise
- disclose the names of any alternative accounts or future accounts to plaintiffs
- allow plaintiffs, through their attorneys, access to copy and inspect the complete transactional records maintained by PayPal, Inc. that were owned or operated by the defendant.

As is evidenced by the above, businesses who operate entirely within a virtual world nevertheless receive recognition of their marks, implying that the mark is "used in commerce" within the definition of the Lanham Act. In fact, Alyssa LaRoche sought and was granted registration of a design mark of an avatar by the U.S. Patent and Trademark Office in connection with virtual content creation

services.[184] This can certainly be seen as a step ahead for trademark rights within virtual media.

It should be noted that Second Life, like Twitter and Facebook, has a policy in place to help avoid infringement and impersonation.[185] Your account name cannot be the name of another individual to the extent that it could cause deception or confusion; a name which violates any trademark right, copyright, or other proprietary right; a name which may mislead other users to believe you to be an employee of Linden Lab; or a name which Linden Lab deems in its discretion to be vulgar or otherwise offensive.[186]

The policy adds that Linden Lab reserves the right to delete or change any account name for any reason or no reason. In addition, an account cannot be transferred without the prior written consent of Linden Lab (however, it will not unreasonably withhold its consent to the transfer of an account in good standing by operation of a valid written will to a single natural person as long as proper notice and documentation are provided as requested by Linden Lab).

The policy further provides that a user shall not:

> (i) take any action or upload, post, e-mail or otherwise transmit Content that infringes or violates any third party rights; (ii) impersonate any person or entity without their consent, including, but not limited to, a Linden Lab employee, or falsely state or otherwise misrepresent your affiliation with a person or entity…[187]

Linden Lab is generally known to remove any content from its site that incorporates another's trademark without the trademark owner's authorization, or features the unauthorized use of celebrity material, as evidenced by the case wherein the Trump organization put Linden Lab on notice that a user was incorporating its "Miss Universe" trademark in its "Miss SL Universe" pageant. Linden Lab put the infringers on notice of the complaint by the Trump organization and proceeded to remove all references to Miss Universe and Miss SL Universe from Second Life. While this is certainly encouraging, the trademark owner or celebrity would be wise to proceed with caution in leaving the determination of what amounts to infringing or unauthorized use to Linden Lab.

The creators of Second Life have also established a Second Life Patent and Trademark Office ("SLPTO") that offers dated evidence of any Second Life creation to help protect the users' intellectual property.[188] While not a legal authority, the SLPTO serves as a neutral third party created to help creators protect their intellectual property, educate them on their rights, and add value to their products. The SLPTO also offers automated DMCA notices, copyright applications, limited edition numbers and individual item registration.

Celebrity Name and Likeness

As noted above, virtual world users create avatars. Many users will fashion an avatar bearing a celebrity's name or likeness. This action results in a separate category of trademark infringement and generates rights of publicity issues, but the results may surprise you. The lead singer of the band Deee-Lite sued Sega of America, Inc. for common law infringement of her right to publicity, misappropriation of her likeness and false endorsement under the Lanham Act (among others), based on the alleged use of her likeness as the basis for a character in one of its video games. Despite the fact that the character bore similar facial features, hairstyle and clothing style, and recited the singer's catchphrase, the court held that there was "sufficient expressive content to constitute a 'transformative work,'" protected under the First Amendment.[189] In a separate avatar-related case, Marvel sued NCSoft for copyright and trademark infringement on the basis that the avatars created in its "City of Heroes" game were "identical in name, appearance and characteristics belonging to Marvel."[190] The case settled.

As these cases evidence, trademark owners and providers of virtual world platforms remain ever vigilant of the growing concern regarding the unauthorized use of trademarks and likenesses. It is in the best interests of both parties to work together in protecting the trademark owners' rights in order to avoid costly and preventable litigation.

Bottom Line—What You Need to Do

It is of the utmost importance to have strategy in place in order to best protect your ownership of intellectual property. By aggressively policing your trademarks, service marks, trade names and copyrights, intellectual property owners will be in the best position to prevent claims that they have waived their ability to enforce their ownership rights, while at the same time discouraging others from any authorized use of your marks and works authorship.

— Biographies of Authors and Editors —

Christopher P. Bennett, Partner – Chicago · +1 312 207 3871 · cbennett@reedsmith.com

Chris joined Reed Smith in 2007, and practices in the firm's Corporate & Securities group. He has extensive experience in a wide variety of transactions, including public securities offerings, private placements of securities (144A and Regulation D), private equity investments and corporate mergers and acquisitions (public and private). Chris represents investment banks and issuers in public and private offerings of equity and debt, and investors and issuers in private equity investments. Chris also represents public companies regarding 34 Act compliance and general corporate matters.

Darren B. Cohen, Partner – New York · +1 212 549 0346 · dcohen@reedsmith.com

Darren provides counsel to advertising agencies and brand owners on all matters of trademark and copyright law, including clearance, prosecution, licenses, assignments, settlement agreements, and domain name disputes, as well as Customs issues. In addition, Darren has overseen the establishment and maintenance of programs designed to secure and protect thousands of domestic and international trademarks. Darren is recommended for his experience on the brand strategy front and for advising advertising clients on trademark matters by *The Legal 500* directory since 2007. According to *The Legal 500 – United States* (2009 Edition), Darren is the driving force behind the trademark group, offering counseling to a multitude of advertising agencies and brand owners on all matters of trademark law.

Amy J. Greer, Partner – Philadelphia/New York · +1 215 851 8211 · agreer@reedsmith.com

Amy joined Reed Smith in 2008 and is a partner who divides time between the firm's Philadelphia and New York offices. She serves as co-leader of the Securities Litigation and Enforcement practice, a component of the Global Regulatory and Enforcement group. Before joining Reed Smith, Amy served as Regional Trial Counsel in the Philadelphia Regional Office of the United States Securities and Exchange Commission. In that role, Amy served as the chief litigation counsel in the Philadelphia office and managed a staff of lawyers responsible for a wide variety of enforcement matters. Amy, an experienced trial lawyer, joined the Agency in July 2003, from private practice, where as a Partner in a large regional law firm, she specialized in complex commercial and corporate litigation.

Gregory J. Hessinger, Partner – New York · +1 212 549 0228 · ghessinger@reedsmith.com

Greg is a partner in the Labor and Employment Group. Greg represents a diverse group of clients in the advertising, entertainment and media industries, including movie studios, television networks, talent agencies, advertisers and major record labels. Greg was previously Executive Director of the Screen Actors Guild (SAG), a 120,000-member national labor union representing actors and other performers. Before that, he was Executive Director of the American Federation of Television and Radio Artists (AFTRA), and earlier still, was the Director of Labor Relations for CBS.

John L. Hines, Jr., Partner – Chicago · +1 312 207 3876 · jhines@reedsmith.com

John is a partner in Reed Smith's Chicago office, where he concentrates his practice in the areas of intellectual property, Internet law and software licensing (including open source). John regularly counsels clients on technology and computer-driven liability, in matters involving unfair competition, copyright infringement, privacy and online speech and defamation (as well as matters involving the U.S. Communications Decency Act). He also advises businesses on policies and practices relating to reputation

management; social media; and generally to the dissemination of content in an electronic environment, including privacy and security policies, website agreements, communications policies and document retention policies.

Andrew L Hurst, Partner – Falls Church/Washington, D.C. · +1 202 414 9275 · ahurst@reedsmith.com

Andrew is a member of Reed Smith's Global Regulatory Enforcement Group. His practice can be described as having three aspects. First, Andrew represents corporations in civil fraud litigation, with a focus on health care providers and other government contractors being sued under the civil False Claims Act. Second, Andrew represents corporations and individuals in connection with criminal investigations and prosecutions by the Department of Justice and other federal and state entities. Third, Andrew serves as outside general counsel for several small and mid-size emerging corporations. He provides general legal advice and facilitates representation of the clients by the appropriate Reed Smith departments, providing these clients with tools to grow to the next level of their business.

Antony B. Klapper, Partner – Washington, D.C. · +1 202 414 9302 · aklapper@reedsmith.com

Tony's practice focuses on products liability, toxic tort and consumer fraud claims, but his litigation experience also includes government contracts, complex business, defamation, and employment litigation. Tony is an experienced litigator with first-chair experience, and has taught for several years trial advocacy courses, including those sponsored by the National Institute of Trial Advocacy and Equal Justice Works.

Joseph I. Rosenbaum, Partner – New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe chairs Reed Smith's global Advertising Technology & Media Law practice and is a partner resident in New York. Joe has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

Carolyn H. Rosenberg, Partner – Chicago · +1 312 207 6472 · crosenberg@reedsmith.com

Carolyn joined Reed Smith when the firm combined with Sachnoff & Weaver. She is a member of the firm's Executive Committee, as well as the firm's Audit Committee, and heads the firm's Talent Committee. She frequently advises corporations, directors and officers, risk managers, insurance brokers, lawyers and other professionals on insurance coverage, corporate indemnification, and litigation matters nationwide and internationally. Carolyn also assists clients in evaluating insurance coverage and other protections when negotiating transactions and represents them in resolving coverage disputes. She has addressed coverage issues ranging from directors' and officers' liability and fidelity bond insurance to data privacy and cyberliability policies. Carolyn is also a frequent speaker and commentator.

Casey S. Ryan, Partner – Pittsburgh · +1 412 288 4226 · cryan@reedsmith.com

Casey is a partner in the Labor and Employment group. She represents employers in a wide variety of employment-related litigation, including harassment, retaliation, discrimination, wrongful discharge and breach of contract litigation in federal courts throughout the country, and routinely appears before both federal and state agencies, including the Equal Employment Opportunity Commission and various state human relations commissions. Casey has prevailed in numerous arbitration proceedings, involving matters such as breach of employment contracts, wage claims and bonus and incentive pay disputes. As part of counseling employers on day-to-day issues, Casey routinely advises on issues of hiring, disciplining and firing in both unionized and non-unionized workplaces. She also routinely advises employers, drafts policies and conducts workforce training on topics such as computer and Internet usage, employee use of social media, employment agreements and handbooks, drug testing and workplace violence.

Alexander "Sandy" Y. Thomas, Partner – Falls Church/Washington, D.C. · +1 703 641 4276 · athomas@reedsmith.com

Sandy focuses his practice on commercial litigation, with particular experience in antitrust counseling and litigation. He has successfully defended clients accused of monopolization and attempted monopolization, trade secrets misappropriation, and violations of state and federal unfair competition laws. He has also represented clients in investigations and enforcement actions brought by U.S. competition agencies. Sandy regularly counsels businesses in claims arising out of breach of contract, including breaches of restrictive covenants and proprietary information agreements. He has litigated such cases to successful bench and jury verdicts. Sandy also has considerable experience advising corporate counsel on issues relating to the attorney-client privilege and the work product doctrine, and has written and spoken extensively on the subjects. He has counseled numerous large corporate law departments on privilege and work-product challenges in internal investigations.

Douglas J. Wood, Partner – New York · +1 212 549 0377 · dwood@reedsmith.com

Douglas Wood. Doug is Chair of Reed Smith's Media & Entertainment Law Group and is resident in the firm's New York office. Doug has more than 30 years' experience representing the entertainment and media industries, including individuals and multinational companies in motion picture, publishing, advertising, marketing, promotions, unfair competition, intellectual property, and e-commerce matters. He is the author of the book, *Please Be ADvised, the Legal Guide for the Advertising Executive*, published by the Association of National Advertisers (www.ana.net) and is the Chairman and founder of the Global Advertising Lawyers Alliance (www.gala-marketlaw.com).

Jesse J. Ash, Associate – Washington, D.C. · +1 202 414 9255 · jash@reedsmith.com

Jesse is a member of the Life Sciences Health Industry Group, practicing in the area of product liability litigation. His practice focuses on products liability and the defense of pharmaceutical and medical device companies in complex actions in state and federal courts. As national counsel for a six state region for one of the largest pharmaceutical companies in the United States, Jesse has overseen hundreds of lawyers, organizing thousands of cases through discovery and trial. He has also represented health care clients on a wide-range of compliance issues, subpoena responses and large-scale civil action discovery responses. As an experienced product liability litigator, Jesse is acutely aware of the benefits and risks involved when companies in the health care industry use social media to market their products.

Paul Bond, Associate – Princeton · 1 609 520 6393 · pbond@reedsmith.com

Paul is a member of the Global Regulatory Enforcement Group, practicing in the areas of data privacy, security, and management. Paul helps our clients comply with legal requirements for the protection of personal data, whether those requirements arise from contract, state, national, or international law. In that vein, Paul counsels clients on how to meet their obligations under, *e.g.*, the Gramm-Leach-Bliley Act, HIPAA, the Fair Credit Reporting Act and its Identity Theft Red Flags regulations, and the dozens of other federal and state privacy law and regulations. Paul has also been actively involved in the successful defense of several dozen putative class actions concerning consumer privacy. Paul is a member of the International Association of Privacy Professionals.

Maureen C. Cain, Associate – Philadelphia · +1 215 851 8294 · mcain@reedsmith.com

Maureen joined Reed Smith in fall 2006 and is a member of the firm's Commercial Litigation Practice Group. She has represented clients at all levels in federal and state court in a wide variety of matters. She has been involved in all aspects of strategic planning, both before and after litigation has commenced, and has experience in all phases of litigation from pre-trial discovery through trial. She has successfully defended a number of clients in lawsuits involving employment discrimination, civil rights, white collar crime, products liability, and financial services issues.

Daniel Z. Herbst, Associate – Washington, D.C. · +1 202 414 9232 · dherbst@reedsmith.com

Dan is an associate in the firm's Global Regulatory Enforcement Group. His experience involves representing clients in a variety of multi-jurisdictional commercial and regulatory litigation. Dan's practice focuses on two practice areas: first, financial services litigation, where he defends banks and other financial institutions in a disputes ranging from large class action litigation to arbitrations before financial regulatory bodies; second, media and defamation law, where he advises clients and litigates disputes relating to broadcast, print, and Internet speech and trade libel and business defamation.

Janice D. Kubow, Associate – New York · +1 212 205 6122 · jkubow@reedsmith.com

Janice is an associate in Reed Smith's New York office. She has extensive experience in a variety of commercial, complex and multi-district litigation matters on behalf of companies in the pharmaceutical, manufacturing and media industries. She has been involved in all aspects of strategic planning, both before and after litigation has commenced, and has extensive experience in all aspects of pre-trial discovery and motion practice, including all phases of expert discovery, electronic discovery and deposition discovery. Janice also counsels on unique issues involving word-of-mouth marketing on digital media platforms, including unfair competition and false advertising, online speech and defamation (as well as matters involving the U.S. Communications Decency Act), cyber-smearing and astroturfing.

Stacy K. Marcus, Associate – New York · +1 212 549 0446 · smarcus@reedsmith.com

Stacy is an associate in the Advertising, Technology & Media Group. She concentrates her practice in e-commerce, advertising and technology law. Stacy advises clients on social media guidelines, branding, trademark and copyright-related issues, celebrity endorsement and talent agreements, software licensing and development, sweepstakes and promotions, mobile marketing, email marketing and telemarketing. She has counseled clients in a wide variety of services available through the Internet and mobile platforms, including issues related to social media, user-generated content and premium SMS promotions. Her clients include advertisers, advertising agencies, financial institutions and website owners.

Amy S. Mushahwar, Associate – Washington, D.C. · +1 202 414 9295 · amushahwar@reedsmith.com

Amy is an associate in the firm's Advertising, Technology & Media Group. She practices in the telecommunications field, primarily in the areas of media, privacy, data security, and emerging technologies. She has experience advising clients, including telecommunications providers, broadcasters, and other business entities, with matters pending before the Federal Communications Commission (FCC), National Telecommunications and Information Administration (NTIA), U.S. Congress, Federal Trade Commission (FTC), and federal courts. Amy represents media clients with regulatory issues spanning media ownership to closed captioning, and channel carriage negotiations to content regulations. As a former technology consultant, Amy also assists technology clients with the development of Service Level Agreements, data security planning and various forms of privacy policies.

Meredith D. Pikser, Associate – New York · +1 212 521 5432 · mpikser@reedsmith.com

Meredith concentrates her practice on intellectual property issues. Her experience includes advising clients in matters relating to trademark, unfair competition, infringement, anti-counterfeiting and domain name disputes. She assists clients in developing and maintaining their intellectual property rights, both foreign and domestic, with special emphasis on trademark clearance and availability, filing and prosecution of trademark applications, opposition and cancellation proceedings, and trademark infringement. Meredith has successfully prosecuted Uniform Domain Name Dispute Resolution Policy actions and advises clients on matters pertaining policing trademarks on social media networks.

Amber M. Spataro, Associate – New York · +1 212 549 0205 · aspataro@reedsmith.com

Amber has extensive experience in all areas of labor and employment law, including employment litigation, advice and counseling, and traditional labor disputes. Amber has litigated various types of employment discrimination claims, wage and hour claims (including class actions), and other employment-related claims (such as breach of contract, defamation, invasion of privacy and unfair competition claims) on behalf of employers in federal and state court at the trial and appellate court levels. Her advice and counseling experience includes Fortune 500 companies as well as small, five-person employers. Amber has assisted in negotiating collective bargaining agreements in various industries. She has also defended against numerous charges, complaints and representation petitions before the NLRB. She specializes in all aspects of union avoidance from restricting union access for the solicitation of authorization cards to successfully petitioning the NLRB to overturn unfavorable election results. Before joining Reed Smith, Amber spent most of her career working for the entertainment industry defending major studios and networks in litigation and providing advice and counsel on various issues unique to the industry.

Jacob Thride, Associate – Chicago · +1 312 207 3888 · jthride@reedsmith.com

Jacob Thride is an associate in Reed Smith's Corporate & Securities Group. Jacob represents a variety of public and private companies, focusing his practice on capital markets, mergers and acquisitions, private equity, venture capital and general corporate matters. Jacob is an associate board member of the Chicago Committee on Minorities in Large Law Firms and a founding member and director of the United Foundation for the Future of Kids.

Anthony S. Traymore, Associate – New York · +1 212 549 0358 · atraymore@reedsmith.com

Anthony provides strategic counsel and transactional support in connection with initiatives involving technology, advertising and media (and the convergence of these sectors) to global and domestic clients across many industries, including media & entertainment, financial services, insurance, retail, consumer brands and hospitality. Anthony has particular expertise counseling clients on issues arising out of the use of social media, digital media and user-generated content both as marketing and communication tools and content delivery platforms.

— Guide to Social Media Terminology and Websites —

Please note that websites are provided in parentheses.

Site Guide

Unless otherwise indicated, the definition provided below has been taken from the website of the social media tool described.

Tools

Bebo – A social networking site that combines community, self-expression and entertainment. The acronym stands for Blog Early, Blog Often. (www.bebo.com)

Facebook – A social utility that connects people with friends and others who work, study and live around them. The site is used by people and businesses to connect with friends, share photos, and create personalized profiles. (www.facebook.com)

Fast Pitch! – A social network for business networking professionals to market their business, press, blogs, events and networks. (www.fastpitchnetworking.com)

Friendster – A global social network emphasizing genuine friendships and the discovery of new people through friends. Online adults, 18-and-up, choose Friendster to connect with friends, family, school, social groups, activities and interests. (www.friendster.com)

Gather – A social networking site that brings people together through the things they love to do and want to talk about. (www.gather.com)

Kickapps – A site that provides brands, enterprises and web publishers with solutions that enable them to create and manage next generation web experiences that are social, interactive, dynamic, distributed, and data-informed. (www.kickapps.com)

LinkedIn – An interconnected network of experienced professionals from around the world. Users can find, be introduced to, and collaborate with qualified professionals who they need to work with to accomplish their goals. (www.linkedin.com)

MOLI – A mall of online stores, where buyers of goods and services can interact directly with the sellers in an environment built exclusively for them. (www.moli.com)

MySpace – An online community that lets users meet their friends' friends. It is used for friends who want to talk online, singles who want to meet other singles, families who want to keep in touch, business people interested in networking, and anyone looking for long-lost friends. (www.myspace.com)

Ning – A social media site built to allow users to explore interests, discover new passions, and meet new people around a shared pursuit. Allows users to create and join new social networks for their interests and passions. (www.ning.com)

Orkut – An online community designed to make the user's social life more active and stimulating. Its social network can help users maintain existing relationships with pictures and messages, and establish new ones by reaching out to people they've never met before. (www.orkut.com)

Plaxo – A social media site that keeps its users connected to the people they know and care about, by using "Pulse," which is a way for the users to see what their friends are posting to other sites, such as their blog, Flickr, Twitter and Yelp. It is also used to securely host address books. (www.plaxo.com)

Publishing

Blogger – A site that provides an easy way for users to share their thoughts about current events, what's going on in their lives, or anything else they'd care to discuss with the world. (www.blogger.com)

Constant Contact – A site that helps all types of small businesses and organizations create professional-looking email newsletters and online surveys. (www.constantcontact.com)

Joomla – A content management system (CMS) that enables the user to build websites and powerful online applications. A content management system is software that keeps track of every piece of content on a user's website, much like a local public library keeps track of books and stores them. (www.joomla.org)

Knol – A user-generated site that makes it easy for anyone to write and share his or her knowledge with the world. Each knol (unit of knowledge) is searchable through popular search engines and is owned by each individual author. (http://knol.google.com/k)

SlideShow – A social entertainment company that offers people the ability to communicate, engage and have fun with one another within the context of relationships they built on social networks such as Facebook and MySpace. (www.slide.com)

TypePad – A blogging service for professionals and small businesses. TypePad hosts many popular blogs and small business websites. (www.typepad.com)

Wikia – A consumer publishing platform where users go to discover, create and share information on thousands of topics. Wikia content is released under a free content license and operates on the Open Source MediaWiki software. (www.wikia.com)

Wikipedia – A multilingual, web-based, free-content encyclopedia project based mostly on anonymous contributions. The name "Wikipedia" is a portmanteau of the words wiki (a type of collaborative website) and encyclopedia. (www.wikipedia.org)

WordPress – A semantic personal publishing platform with a focus on aesthetics, web standards, and usability. It is used as a blog publishing application and content management system. (www.wordpress.org)

Photos

Flickr – An online photo management and sharing application. It has two main goals, which are to help people make their content available to the people who matter to them, and to enable new ways of organizing photos and video. (www.flickr.com)

Photobasket – An online storage site for users' photos. (photobasket.co.cc)

Photobucket – A site that offers image hosting, free photo-sharing and video-sharing. Allows users to upload photos, host their videos, and share them with friends and family. (photobucket.com)

Picasa – A free software download from Google that helps users organize, edit, and share photos. (picasa.google.com)

Radar – A way to instantly share camera phone pictures, videos and conversations between friends. Radar is free and works on any mobile phone. (radar.net)

SmugMug – A photo- and video-sharing site, which allows users to easily create online photo albums, and share, store, organize and print. (www.smugmug.com)

Twixtr – A site that allows users to share pictures from their mobile phone and automatically publish them on social networks and photo-sharing sites. (www.twitxr.com)

Zooomr – A social utility for friends, family and co-workers who want to communicate securely through both photos and text messages in real-time. (www.zooomr.com)

Audio

iTunes – A free application for Mac or PC users, which organizes and plays their digital music and video on their computer. It syncs all media with their iPod, iPhone, and Apple TV. They can also purchase entertainment for their iPod touch, iPhone, and Apple TV. (www.apple.com/itunes)

Podbean – A website to host and socially subscribe to podcasts on. Podcast Social Subscribing lets the user collect his or her favorite podcast in one place and find everyone else's favorites. (www.podbean.com)

Podcast.com – A podcast destination that provides access to a growing list of more than 60,000 constantly updated podcast feeds representing more than 1 million episodes of audio and video content. (www.podcast.com)

Rhapsody – A digital music service that lets users listen to a variety of music by paying for a membership rather than per track. (www.rhapsody.com)

Video

Brightcove – An online video platform used by media companies, businesses and organizations worldwide to publish and distribute video on the web. Its on-demand platform is used by hundreds of professional publishers to power online video initiatives that reach more than 100 million Internet users every month. (www.brightcove.com)

Digital Video Recorder (DVR) – A device that records video in a digital format to a memory medium, such as a disk drive, within a device. Source: Wikipedia

Google Video – A website for video posting and sharing. It is provided by Google, so it also offers a video search engine. Source: Wikipedia (video.google.com)

Hulu – A free online video service that offers hit TV shows including "Family Guy,," "30 Rock," and the "Daily Show with Jon Stewart." (www.hulu.com)

Metacafe – A video site attracting more than 40 million unique viewers each month. It specializes in short-form original content– from new, emerging talents and established Hollywood heavyweights alike. (www.metacafe.com)

Viddler – A service that allows a user to upload videos, record videos directly to the site via webcam, post comments and tags at specific points in the video, and share videos with RSS and iTunes. (www.viddler.com)

YouTube – A website for users to upload and share video. It uses Adobe Flash Video technology to display content that is uploaded by users, such as movie clips, TV clips, music videos and video blogging. Source: Wikipedia (www.youtube.com)

Microblogging

Plurk – A way to chronicle and share the things users do, the way they feel, and all the other things in between that make up their life. (www.plurk.com)

Twitter – A social networking and micro-blogging site that allows users to send and read messages from others they follow. A tweet is an individual post to Twitter of up to 140 characters, which is then displayed in the writer's profile page and delivered to their subscribers, also known as followers. Source: Wikipedia (www.twitter.com)

Twitxr – A site that allows users to share pictures from their mobile phone and automatically publish them on social networks and photo-sharing sites. (www.twitxr.com)

Livecasting

BlogTalkRadio – A site that allows users to create free talk radio podcasts and listen to thousands of original talk radio shows. (www.blogtalkradio.com)

Live365 – A site that offers a depth of streaming music, talk, and audio, and that features 260+ genres of music produced by 5,000+ broadcasters and music tastemakers from more than 150 countries. Through easy-to-use tools and services, as well as royalty coverage, anyone with a computer and Internet connection can create his or her own Internet radio station and reach a global audience. (www.live365.com)

Justin.tv – An online community for people to broadcast, watch and interact around live video. (www.justin.tv)

SHOUTcast – An Internet radio service that offers free MP3 & AAC radio stations from DJs and broadcasters around the world. (www.shoutcast.com)

TalkShoe – A service that enables anyone to easily create, join, or listen to live interactive discussions, conversations, podcasts and audioblogs. (www.talkshoe.com)

Virtual Worlds

Active Worlds – A site that offers a comprehensive platform for delivering real-time interactive 3-D content over the web. Businesses can use it to sell products, perform interactive product demos, and conduct online corporate training. (www.activeworlds.com)

Kaneva – A site that combines social network with a virtual world. Members create the digital version of themselves, known as avatars, and then meet up in a 3-D world based on the modern day, where they can listen to music, shop and invite friends to their virtual loft. (www.kaneva.com)

Second Life – A free 3-D virtual world where users can socialize, connect and create using voice and text chat. (www.secondlife.com)

There – An online getaway where members can hang out with their friends and meet new ones in a 3-D environment. (www.there.com)

ViOS (Visual Internet Operating System) – A way of organizing all Internet resources, including web pages, into multiuser 3-D environments. These environments include customizable avatars for the users. Source: Wikipedia

Gaming

Entropia Universe – A multiplayer virtual world that has no subscription fees, but members buy in-game currency with real money to buy virtual items. Source: Wikipedia (www.entropiauniverse.com)

EverQuest – A multiplayer online game in which members create a character, such as an elf or a dwarf, select their occupation, and fight monsters and enemies for treasure and experience points. They can also interact with other players through role-playing. Source: Wikipedia (everquest.station.sony.com)

Halo3 – A first-person shooter online and console (Xbox) game for 1-16 players. It represents the third chapter in the Halo trilogy, in which players engage in combat in a mysterious alien ring-world. (www.halo.xbox.com/halo3)

World of Warcraft – A multiplayer online role-playing game, which is often referred to as WoW. Members create a character, explore, fight monsters, complete quests and interact with other members. Source: Wikipedia (www.worldofwarcraft.com)

Productivity

Acteva – An event-registration service-provider for event organizers. It automates the entire event-registration process and brings it online where it can be easily accessed any time. (www.acteva.com)

AOL – A global web services company with an extensive suite of brands and offerings. The business spans online content, products, and services that the company offers to consumers, publishers and advertisers. (www.aol.com)

Avvo – A website that rates and profiles lawyers. It also allows users to review attorneys based on their experience with them. (www.avvo.com)

BitTorrent – An open source file-sharing application effective for distributing very large software and media files. (www.bittorrent.com)

Concep – An interactive email marketing platform. It allows users to create digital email campaigns and view statistics on readership. (www.concepglobal.com)

Constant Contact – A site that helps organizations create professional-looking email newsletters and online surveys. (www.constantcontact.com)

Eventful – An events website that enables its community of users to discover, promote, share and create events. (www.eventful.com)

Google Alerts – A service that provides email updates of the latest relevant Google results (web, news, etc.) based on the user's choice of query or topic. (www.google.com/alerts)

Google Docs – A web-based word processor and spreadsheet, which allows users to share and collaborate online. (docs.google.com)

Google Gmail – An email provider that is built on the idea that email can be more intuitive, efficient and useful. (mail.google.com)

MSGTAG (Message Tag) – An email-tracking program that tracks whether or not a user's sent email has been read. (www.msgtag.com)

ReadNotify – A program in which users get free return email notifications, and/or SMS/ICQ instant messages when email they have sent gets opened, and they can track their emails' reading history. (www.readnotify.com)

Sensidea – A digital media consultancy and products company that helps clients deliver innovative digital strategies, products, and solutions. (www.sensidea.com)

SurveyMonkey – A tool to create and publish custom surveys, and then view results graphically and in real time. (www.surveymonkey.com)

TiddlyWiki – A reusable, non-linear personal notebook. It is the place to find documentation and resources from TiddlyWiki users and developers. (www.tiddlywiki.org)

Yahoo! – An online network of integrated services that allows users to communicate with each other, conduct transactions, and access, share and create information. (www.yahoo.com)

Zoho – A comprehensive suite of online business applications. Customers use Zoho to run their business processes, manage their information, and be more productive while at the office or on the go. (www.zoho.com)

Zoomerang – An online survey software tool that allows users to create online surveys while providing reporting and advanced survey logic. (www.zoomerang.com)

Aggregators

Delicious – A social bookmarking service that allows users to tag, save, manage and share web pages from a centralized source. (www.delicious.com)

Digg – A place for people to discover and share content from anywhere on the web. From the biggest online destinations to the most obscure blog, Digg surfaces the best stuff as voted on by its users. (www.digg.com)

FriendFeed – A service that allows users to invite friends, and get an instant, customized feed made up of the content that their friends share, from photos to interesting links and videos, to messages just for them. (www.friendfeed.com)

Google Reader – A site that constantly checks a user's favorite news sites and blogs for new content. It shows the user all of his or her favorite sites in one place. (www.google.com/reader)

iGoogle – A service that allows users to add news, photos, weather, and other items from across the web to their page. (www.google.com/ig)

Mixx – A user-driven social media website that serves to help users submit or find content by peers based on interest and location. Source: Wikipedia (www.mixx.com)

My Yahoo! – A customizable web page with news, stock quotes, weather, and many other features. (my.yahoo.com)

Reddit – A source for what's new and popular online. The users vote on links that they like or dislike and help decide what's popular, or submit their own links. (www.reddit.com)

SocialSeek – A product of Sensidea, which lets users search for a topic, item, brand or company across news sites, blogs, Twitter, YouTube, Flickr, and events. The user can also track mentions of a particular search query by city and receive charts that show trends on popularity of a topic across websites, or Twitter. (www.sensidea.com/socialseek/download.html)

StumbleUpon – A service that helps the user discover and share websites with others who have similar interests. It allows users to rate websites and recommend sites to friends. (www.stumbleupon.com)

Yelp – An online urban city guide that helps people find places to eat, shop, drink, relax and play, based on the informed opinions of a vibrant and active community of locals in-the-know. (www.yelp.com)

RSS (Rich Site Summary)

Atom – A way to read and write information on the web, allowing users to keep track of more sites in less time, and to share their words and ideas by publishing to the web. (www.atomenabled.org)

FeedBurner – Gives weblog owners and podcasters the ability to manage their RSS feeds and to track usage of their subscribers. (www.feedburner.com)

PingShot – A feature of FeedBurner that alerts users that new content is on a particular feed. Source: Google.com (www.feedburner.com/fb/a/publishers/pingshot)

RSS 2.0 – A web-feed format that publishes content, such as blog entries, news, audio and video. It includes full and summarized text and published dates and authors. Source: Wikipedia

Search

Bing – A search engine that finds and organizes the answers users are looking for so they can make faster, better-informed decisions. (www.bing.com)

EveryZing – A digital media merchandising platform, in which media companies leverage EveryZing's ability to drive the volume of online content consumption and create new revenue streams. (www.everyzing.com)

Google Search – A search engine that allows users to seek out content on the web. (www.google.com)

IceRocket – A search engine that specifically searches blogs and other sources, such as Twitter and MySpace. Source: Wikipedia (www.icerocket.com)

MetaTube – A website to browse the top 100 of the most popular video-sharing sites around the world related to any topic. The user only needs to enter his or her specific search term once for all 100 sites to appear. (www.metatube.net)

Redlasso – A site that enables users to search nearly live TV and radio. Users can search for clips, create clips of the stories, and share them with friends. (www.redlasso.com)

Technorati – A blog search engine that also provides services to the blogs and social media sites, and connects them to advertisers who want to join the conversation. (www.technoratimedia.com)

Yahoo! Search – A web search engine that assists users in finding what they are looking for. (search.yahoo.com)

Mobile

airG – A service that powers mobile communities and wireless social networking. It has a worldwide mobile community and interconnects with mobile operators, such as Sprint Nextel, AT&T and Vodafone. (www.airg.com)

AOL Mobile – A service that allows users to receive news, email, and instant messages via their mobile phone. (http://mobile.aol.com/)

Brightkite – A social networking site that connects people based on the places they visit in the real world. With Brightkite, users can see where their friends are, what they're up to, see what's going on around them, and meet real-world friends. (www.brightkite.com)

CallWave – A provider of Internet and mobile-based unified communications solutions. These solutions allow mobile professionals to communicate and collaborate from anywhere and from any device. (www.callwave.com)

Jott – A site that allows individuals and businesses to easily capture thoughts, send emails and text messages, set reminders, organize lists, and post to web services and business applications–all with their voice, using any phone. (www.jott.com)

Jumbuck – A provider of community messaging applications to wireless carriers. (www.jumbuck.com)

SMS.ac – A mobile data and Internet communications company that distributes and bills people purchasing and selling content, such as video, music and applications, through mobile devices. Source: Wikipedia (www.sms.ac)

Interpersonal

Acrobat Connect – A web conferencing software that allows users to communicate and collaborate instantly through interactive online personal meetings. (www.adobe.com/products/acrobatconnect)

AOL Instant Messenger – A program where users can send messages to friends instantly and keep track of friends' status and presence updates. (www.aim.com)

Go To Meeting – A web conferencing software that allows users to work with anyone, anywhere, in online meetings. (www.gotomeeting.com)

iChat – An instant messaging application that works with AIM (AOL Instant Messenger) and helps users stay in touch with friends using text and video. (www.apple.com/support/ichat/)

Jott – A site that allows individuals and businesses to easily capture thoughts, send emails and text messages, set reminders, organize lists, and post to web services and business applications–all with their voice, using any phone. (www.jott.com)

Meebo – A web platform for IM (Instant Messaging) on any network or site. It connects the user to MSN, Yahoo, AOL/AIM, MySpace, Facebook, Google Talk, and others. (www.meebo.com)

Skype – A program that allows users to make free calls over the Internet to other people for an unlimited time period, to anywhere. It is free to download. (www.skype.com)

Webex – A program that provides users with online meetings, desktop sharing, web conferencing, video conference, net meeting, and web conference. It combines real-time desktop sharing with phone conferencing. (www.webex.com)

Terminology

Advercasting – A term to describe advertising on a podcast or video podcast. Source: Wikipedia

Advergaming – A term to describe the act of playing an advergame, which is a computer game published by an advertiser to promote a product or service. Source: Wikipedia

Astroturfing – A term used to describe an advertising, public relations or political campaign that is planned by an organization, but designed to mask the origin and create the impression of being spontaneous, or to mask statements by third parties. Fake reviews posted on product sites would be examples of astroturfing. Source: Wikipedia

Blog – A type of website in which entries are usually made regularly by one person, containing commentary, descriptions of events, or other materials such as graphics or video. The term blog can also be used as a verb, meaning to uphold or add substance to a blog. Source: Wikipedia

Bookmark – Also known as a favorite, it is a term to describe a record of the address of a file or webpage serving as a shortcut to it, or the act of creating a bookmark to easily access it at a later time. Source: Wikipedia

Buzz Marketing – A term used to describe word-of-mouth marketing. The interaction of users of a product or service amplifies the original marketing message, creating a form of hype. Source: Wikipedia

Computer-Generated Imagery (CGI) – The application of the field of computer graphics, such as 3-D computer graphics to special effects in films, television programs, commercials, simulators and simulation generally, and printed media. Source: Wikipedia

Cybersmearing – A term describing the insulting of an individual or company online. Source: www.goliath.com

Digital Download – A method of retrieving web content, such as games, music, videos, etc., via downloading from a particular source.

Embedded Players, Widgets and Gadgets – Tools that are added and set in to a webpage. For example, a blog can have an embedded widget allowing users to follow Twitter events on their webpage. Source: Wikipedia

Interactive Gaming – An electronic game that involves interaction with a user interface and usually other users via instant messages or voice chat, such as World of Warcraft or Webkins. Source: Wikipedia

Interstitial Advertisement – A webpage of advertising that displays before the user's expected content page. Source: Wikipedia

Keyword – A term used to locate material in a search engine or catalog. Source: Wikipedia

Meta Tag – A tool used by content-owners to communicate information about their webpage to search engines, such as a description tag with text, that is to appear in major search engine directories that describes the site or the use of a keyword tag to help push information to end-users via search engine results when they are seeking material related to those words. Source: Wikipedia

Microsode – A relatively short video of content to be viewed, usually over the Internet.

Mobisode – An episode of content that has been condensed to be viewed with a cellular phone. Source: Wiktionary

On-Demand Programming – A term to describe the systems, Video on Demand or Audio Video on Demand, which allow users to select and watch and/or listen to video or audio content at their request. Source: Wikipedia

Opt In – A term to describe when someone is given the option to receive "bulk" email. Obtaining permission before sending email is critical because without it, the email is Unsolicited Bulk Email, known as spam. Source: Wikipedia

Opt Out – A term to describe the method by which an individual can avoid receiving unsolicited product or service information. Source: Wikipedia

Podcast – A series of digital media files (either audio or video) that are released regularly and downloaded through web syndication. Special client software applications that are used to deliver the podcasts (i.e., iTunes, Zune, Juice and Winamp) are what differentiates podcasts from other ways of accessing media files over the Internet. Source: Wikipedia

Promercial – A term to describe on-air promotion spots, with brands increasingly being incorporated into these tune-in spots on many networks. Source: www.allbusiness.com

Satellite Dish – A type of antenna designed to receive microwaves from communications satellites that transmit data or broadcasts, such as satellite television or radio. Source: Wikipedia

Search Engine – A tool to search for information on the World Wide Web. Source: Wikipedia

SMS (Short Message Service) – A service for sending text messages by way of a cellular telephone, usually mobile-to-mobile. Source: Wiktionary

Social Networking – A term to describe the act of making connections and socializing with people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social networking is done through web-based programs, which provide a multitude of ways for users to interact. Source: Wikipedia

Streaming – A method of delivering a medium, such as audio or video content, over telecommunications networks. Source: Wikipedia

Twitter-Jacking – A term describing the act of one person taking control of another person's Twitter account, usually to post untrue or harmful material. Source: www.mashable.com

Typosquatting – Also known as URL hijacking, is a type of cybersquatting when a user accidentally enters an incorrect website address, then is led to an alternative website, usually displaying undesired materials, owned by a cybersquatter. Source: Wikipedia

Unwired or Wireless – A term to describe an electronic device being equipped with Internet or electricity, without the use of electrical conductors or wires. Source: Wikipedia

User-Generated Content – A term that refers to various kinds of publicly available media content, produced by end-users. Also known as consumer-generated media or user-created content. Source: Wikipedia

Viral Marketing – A term that describes marketing techniques that use pre-existing social networks to produce an increase in brand awareness or to achieve other marketing objectives. Source: Wikipedia

Virtual Community – A group of people who primarily interact via electronic media such as newsletter, telephone, email, Internet social network service or instant messages rather than face-to-face, for social, professional, educational or other purposes. Also known as an e-community or online community. Source: Wikipedia

Virtual Reality – A technology that allows a user to interact with a computer-simulated environment, either simulating real world or an imaginary world. Source: Wikipedia

Vlog – The shortened term for video blogging, it's a form of blogging utilizing the video medium. Source: Wikipedia

WAP (Wireless Application Protocol) – An open international standard for network communications in a wireless-communication environment. Most of its use involves the ability to access the mobile web from a mobile phone or PDA. Source: Wikipedia

Webcast – A media file broadcasted over the Internet using streaming media technology. Source: Wikipedia

Wi-Fi – A trademark of the Wi-Fi Alliance, a global, nonprofit association of companies that promotes WLAN technology and certifies products as Wi-Fi-Certified, to ensure compatibility among products that communicate data wirelessly via the IEEE 802.11 specification. Source: Wikipedia

Wired – A term to describe an electronic device being equipped with wires, so as to connect to a power source or to other electric or electronic wires. Source: Wiktionary

Word-of-Mouth Advertising – Promotion of a product or service through oral statements by independent users or individuals authorized by a marketer.

— Endnotes —

1 E-consultancy.com Limited, http://econsultancy.com/blog/4402-20+-more-mind-blowing-social-media-statistics

2 *See*, "Changing the Conversation," http://www.publicis.com/#en-GB/approach

3 http://experiencematters.wordpress.com/2009/09/26/best-buy-learns-social-media-lesson/

4 http://www.youtube.com/watch?v=5YGc4zOqozo

5 NYT October 29, 2009, "With Video, a Traveler Fights Back," http://www.nytimes.com/2009/10/29/business/29air.html

6 http://www.youtube.com/watch?v=-QDkR-Z-69Y&feature=PlayList&p=7EDD98D1C5CD57F6&playnext=1&playnext_from=PL&index=5

7 http://www.dailymail.co.uk/news/worldnews/article-1201671/Singer-Dave-Carroll-pens-YouTube-hit-United-Airlines-breaks-guitar--shares-plunge-10.html

8 http://www.govtrack.us/congress/bill.xpd?bill=s111-213

9 http://static.uspirg.org/consumer/archives/airline_passenger_rights/index.html; *see also* http://www.examiner.com/x-10533-Seattle-Travel-Industry-Examiner~y2009m9d23-Power-to-the-people--airline-passengers-that-is-if-the-Passenger-Bill-of-Rights-gets-passed

10 http://www.youtube.com/watch?v=6cOb7fWG0A0

11 http://www.prweekus.com/Dominos-changes-up-online-strategy-following-video-prank/article/130751/

12 Erik Qualman, http://socialnomics.net/

13 World Internet Usage Statistics, http://www.internetworldstats.com/stats.htm, as of June 30, 2009.

14 Lisa Lacy, "Nielsen: Social Media Ad Spending Up Sharply," ClickZ.com, Sept. 25, 2009.

15 *Id*.

16 *Id*.

17 http://www.facebook.com/terms.php?ref=pf, http://www.youtube.com/t/terms, and https://twitter.com/tos

18 *Id*.

19 http://twitter.zendesk.com/forums/26257/entries/18366#

20 With regard to eligibility, in order to avoid Children's Online Privacy Protection Act ("COPPA") issues, a sponsor should limit eligibility to individuals who are at least the age of majority in the jurisdiction in which they reside (18 in most states). If individuals under the age of 18 are permitted to enter, they should do so only with parental permission. If individuals under the age of 13 are permitted to enter, a company must comply with both the COPPA requirements concerning collection of personal information from children, and Children's Advertising Review Unit ("CARU") requirements for advertising directed toward children. Remember, however, that if a promotion is being offered via a third-party's website or platform (*e.g.*, Facebook, YouTube or Twitter), a company must comply with such third-party's terms of use, which typically prohibit use by children under 13.

21 N.Y. G.B.L. § 369-e and F.L. Stat. § 849.094.

22 *Id*.

23 R.I. Stat. Ch. 11-50, *et seq.*

24 Mark Adams, Director of Communications for the International Olympic Committee, quoted in "Social media bringing down the walled garden of the Olympic Games," TMC.net, Sept. 24, 2009.

25 16 CFR Part 255.

26 16 CFR § 255.l(d).

27 http://fastlane.gmblogs.com

28 http://thelab.gmblogs.com

29 http://fastlane.gmblogs.com/about.html

30 http://thelab.gmblogs.com/about/

31 *Id*.

32 Andrew LaVallee, "Starbucks Unveils Its First iPhone Apps," http://blogs.wsj.com/digits/2009/09/23/starbucks-unveils-its-first-iphone-apps/, Sept. 23, 2009.

33 *Doctor's Associates Inc. v. QIP Holders LLC*, 82 U.S.P.Q.2d (BNA) 1603 (D. Conn. April 18, 2007).

34 This discussion presumes that either the advertiser or advertising agency is a signatory to the union contracts. Of course, if there is no signatory relationship, no contractual obligations will exist, although professional talent may insist upon such contractual coverage.

35 *See,* Cass R. Sunstein, "On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done," (Farrar, Straus, and Giroux 2009).

36 The Impact of the Class Action Fairness Act of 2005 on the Federal Courts.

37 15 U.S.C. § 45.

38 15 U.S.C. § 1125(a).

39 15 U.S.C. § 45.

40 Available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm

41 *Kraft, Inc. v. Federal Trade Commission*, 970 F.2d 311, 314 (7th Cir. 1992); *FTC v. Brown & Williamson Tobacco Corp.*, 776 F.2d 35, 40 (D.C. Cir. 1985).

42 *Int'l Harvester Co*., 104 FTC 949 1058 (1984).

43 *Sandoz Pharmaceuticals v. Richardson-Vicks*, 902 F.2d 222, 228 (3d Cir. 1990).

44 15 U.S.C. § 45 (m)(1)(A) (civil penalty of $10,000 per violation where violator has actual knowledge, or knowledge fairly implied). 15 U.S.C. § 53(b).

45 *U.S. Healthcare v. Blue Cross of Greater Philadelphia*, 898 F.2d 914, 921 (3d Cir. 1990); *Johnson & Johnson v. Carter-Wallace, Inc.*, 631 F.2d 186, 190-91 (2d Cir. 1980).

46 *Sandoz Pharmaceuticals v. Richardson-Vicks*, 902 F.2d 222, 228 (3d Cir. 1990) ("The key distinctions between the FTC and a Lanham Act plaintiff turns on the burdens of proof and the deference accorded these respective litigants. The FTC, as a plaintiff, can rely on its own determination of deceptiveness. In contrast, a Lanham Act plaintiff must prove deceptiveness in court.").

47 *U.S. Healthcare*, 898 F.2d at 921 (3d Cir. 1990) (quoting 2 J. McCarthy, Trademarks and Unfair Competition § 27:713 (2d Ed. 1984)).

48 *See*, *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, available at http://www.ftc.gov/opa/2009/10/endortest.shtm ("FTC Guides") (issued Oct. 5, 2009 and effective Dec. 1, 2009).

49 *See, e.g*., *Ramson v. Layne*, 668 F.Supp. 1162 (N.D. Ill. 1987).

50 FTC Guides, at 5, n.11.

51 FTC Guides, § 255.0.

52 FTC Guides, at 8.

53 15 U.S.C. § 45.

54 FTC Guides, § 255.1(d).

55 FTC Guides, at 38-39.

56 FTC Guides, § 255.1(d).

57 FTC Guides, at 42.

58 *Id*.

59 FTC Guides, at 15.

60 *Id*.

61 FTC Guides, at 39.

62 FTC Guides, at 40, 42.

63 *See,* 1 McCarthy, *Rights of Publicity*, § 5:22 ("under the proper circumstances, any person, celebrity or non-celebrity, has standing to sue under § 43(a) for false or misleading endorsements."), quoted in *Doe v. Friendfinder Network, Inc*., 540 F.Supp.2d 288, 301 (D.N.H. 2008).

64 540 F.Supp.2d 288 (D.N.H. 2008).

65 *Id.* at 305-306; *see also*, *Ting JI v. Bose Corporation*, 2009 WL 2562663, at *3, No. 06-10946-NMG (D. Mass, Aug. 12, 2009).

66 Restatement, Second, Torts § 558.

67 *Dendrite v. Doe*, 775 A.2d 756, 760 (N.J. App. 2001); *but see*, *Solers, Inc. v. Doe*, 977 A.2d 941, 954 (D.C. 2004) (requiring a prima facie showing but rejecting a balancing test at the end of the analysis); *see also*, *Cohen v. Google, Inc*., No. 100012/09 (Unpublished) (New York Supreme Court orders Google's Blooger.com to disclose identity of anonymous blogger, where plaintiff established the merits of her cause of action for defamation and the information sought was material and necessary to identify potential defendants).

68 *E.g., Stratton Oakmont v. Prodigy*, 1995 WL 323710, at *3 (N.Y. Sup. Ct., May 24, 1995) (Unreported).

69 *E.g., Cubby v. Compuserve*, 776 F.Supp. 135 (S.D.N.Y. 1991).

70 47 U.S.C. § 230 ("CDA").

71 47 U.S.C. § 230(c)(1).

72 47 U.S.C. § 230(f)(3).

73 474 F.Supp. 2d 843 (W.D. Tex. 2007).

74 *Id.* at 849.

75 *See Batzel v. Smith,* 333 F.3d 1018 (9th Cir. 2003) (provider's "minor alterations" to defamatory material not actionable); 318 F.3d 465, 470-71 (3d Cir. 2003); *Ben Ezra, Weinstein & Co. v. Am. Online, Inc.,* 206 F.3d 980, 985-86 (10th Cir. 2000) (rejecting argument that service provider's deletion of some, but not all, inaccurate data about plaintiff from another source "transforms Defendant into an 'information content provider' "); *Blumenthal v. Drudge,* 992 F.Supp. 44, 52 (D.D.C.1998) (exercise of "editorial control" over defamatory third-party content fell within § 230 immunity); *Doe v. Friendfinder Network, Inc*., 540 F.Supp.2d 288, 297 and n. 10 (D.N.H. 2008) (slight editorial modifications to defamatory profile does not defeat immunity).

76 *See*, *Anthony v. Yahoo! Inc.,* 421 F.Supp.2d 1257, 1262-1263 (N.D. Cal. 2006) (service's alleged creation of false profiles inducing plaintiff to maintain his membership not barred by Section 230); *Hy Cite Corp. v. badbusinessbureau.com, L.L.C.,* 418

F.Supp.2d 1142, 1149 (D. Ariz. 2005) (service provider's creation of its own comments and other defamatory content associated with third-party postings defeats Section 230 defense).

77 *Batzel v. Smith,* 333 F.3d 1018 (9th Cir. 2003); *Zeran v. Am. Online, Inc.,* 129 F.3d 327, 330 (4th Cir. 1997) (right to exercise traditional editorial functions, including "whether to publish, withdraw, postpone or alter").

78 540 F.Supp.2d at 295-96 (emphasis in original). *See also*, *Barrett v. Rosenthal*, 50 Cal.4th 33, 146 P.3d 510 (2006) (noting § 230(c)(1) protects any "provider *or user*" (emphasis added), California Supreme Court holds individual user of social media immune from reposting message she received electronically from another "content provider").

79 2009 WL 3240365, No. 102578/09 (N.Y. Sup. Sept. 15, 2009).

80 2009 WL 3240325, at *1.

81 2009 WL 3240365, at *1 (*citing Blumenthal v. Drudge*, 992 F.Supp. 44, 52 (D.D.C. 1998)).

82 478 F.3d 413 (1st Cir. 2007).

83 *Id*. at 421.

84 521 F.3d 1157 (9th Cir. 2008) (*en banc*).

85 *See also, Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc*, 519 F.3d 666, 669-70 (7th Cir. 2008) (rejecting that Section 230 confers an absolute immunity).

86 47 U.S.C. § 230(e)(2).

87 *See, Doe v. Friendfinder Network*, 540 F.Supp.2d at 303 n. 13 (notion that trademark claims are not intellectual property claims, while not before the court, strikes it as "dubious").

88 488 F.3d 1102 (9th Cir.), *cert. denied*, 128 S.Ct. 709 (2007).

89 *Id*. at 1118-19.

90 540 F.Supp.2d 299-304. *Accord*, *Atlantic Recording Corporation v. Project Playlist*, 603 F.Supp.2d 690 (S.D.N.Y. 2009).

91 O'Grady v. Superior Court (Apple Computer, Inc.), 39 Cal.App.4th 1423 (Sixth Dist. 2006).

92 Clifford, "Video Prank at Domino's Taints Brand," http://www.nytimes.com/2009/04/16/business/media/16dominos.html (April 15, 2009).

93 "Press Room," available at: http://www.facebook.com/press/info.php?statistics

94 Callan Green, "Killer Facebook Fan Pages: 5 Inspiring Case Studies," Mashable.com (June 16, 2009) available at: http://mashable.com/2009/06/16/killer-facebook-fan-pages/

95 Lisa Wehr,"Jet Blue & Taco Bell: Lessons in Crisis Marketing," iMediaConnection.com (April 19, 2007), available at: http://www.imediaconnection.com/content/14452.imc

96 John Lister, "Most Departing Employees Steal Company Data," Tech.Blorge (Feb. 23, 2009) available at: http://tech.blorge.com/Structure:%20/2009/02/23/most-departing-employees-steal-company-data/ (stating almost six in 10 people who left a job in the United States in 2008 took confidential data with them, according to a survey by data protection firm Ponemon), and "Many Users Say They'd Sell Company Data for the Right Price," by Tim Wilson, DarkReading (Apr. 24, 2009) available at: http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=217100330 (stating 37 percent of workers would sell data for $1.5 million, according to a survey of commuters in London's railway stations by InfoSecurity Europe).

97 For example, the Gramm-Leach-Bliley Act requires certain types of companies (financial institutions, insurance companies and brokerage companies) to maintain privacy policies.

98 Some common privacy-oriented consumer monitoring groups are: the Electronic Privacy Information Center, Privacy Rights Clearinghouse, World Privacy Forum and the Electronic Frontier Foundation, among others.

99 *See*, Facebook's New Terms of Service: "We Can Do Anything We Want With Your Content. Forever." by Chris Walters, the *Consumerist* (Feb. 15, 2009) available at: http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever

100 *See,* Caroline McCarthy, "MoveOn.org takes on Facebook's 'Beacon' Ads," CNET (Nov. 20, 2009), available at: http://news.cnet.com/8301-13577_3-9821170-36.html

101 *See,* Louise Story and Brad Stone, "Facebook Retreats on Online Tracking," *New York Times* (Nov. 30, 2007), available at: http://www.nytimes.com/2007/11/30/technology/30face.html

102 Sam Diaz,"Beacon Settlement Gets Preliminary Ok," CNET (Oct. 24, 2009), available at http://news.cnet.com/8301-1023_3-10382634-93.html

103 Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers, who are known as followers.

104 The retweet (or "RT" in front of the Twitter line) allows Twitter users to share the best links, tweets, and gems they find from others using the service. These messages can be positive or negative in nature.

105 For "retweets," the company would need to seek removal of the information under Twitter's user agreement, which is available at http://help.twitter.com/forums/26257/entries/18311

106 YouTube Website, Privacy Issues: Privacy Complaints for Other People, available at: http://www.google.com/support/youtube/bin/answer.py?answer=84753 ("In order to process privacy claims, we must receive notification directly from the individual in the video…. Any attempt to report a privacy violation for someone other than yourself will not be investigated.")

107 Facebook Statement of Rights and Responsibilities, available at: http://www.facebook.com/terms.php?ref=pf (last visited, Oct. 27, 2009).

108 *Id.* at § 5.8.

109 MySpace.com Terms of Use Agreement, last updated June 25, 2009, available at: http://www.myspace.com/index.cfm?fuseaction=misc.terms

110 *Id.* at §§ 8.6, 8.16.

111 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

112 Opinion 5/2009 on online social networking, p. 6.

113 "Facebook Won't Face Off with Canada's Privacy Commissioner," 27 No. 9 *Andrews Computer & Internet Litig. Rep.* 11 (Sept. 30, 2009).

114 Portions of this chapter first appeared in, and are reprinted with permission of, the *Privacy & Security Law Journal.*

115 "Facebook Shuts Down Beacon to Settle Class-Action Lawsuit," 27 No. 9 *Andrews Computer & Internet Litig. Rep.* 8 (Sept. 30, 2009), citing *Lane, et al. v. Facebook Inc., et al*., No. 08-CV-03845-RS (N.D. Cal.).

116 http://www.iab.net/insights_research/public_policy/behavioral-advertisingprinciples

117 "Concerned mother sets up MySpace sting operation," 5 No. 7 Quinlan, *Computer Crime and Technology in Law Enforcement* art. 2 (July 2009).

118 "Impeachment by Facebook Status Update?" 14 No. 9 *Cyberspace Law.* 23 (2009), citing to *State v. Corwin*, 2009 WL 2562667 (Mo. App. August 20, 2009) (upholding convicting despite allegation that exclusion of Facebook status page was error).

119 Tariq Remtulla, "Facebook Not So Private? Ontario Court Finds Facebook Profile Discoverable," 14 No. 4 *Cyberspace Law.* 17 (May 2009).

120 Margaret DiBianca, "Warnings Against LinkedIn Recommendations: Justified or Propaganda?" 14 No. 9 Del. Emp. L. Letter 2 (Sept. 2009).

121 Allegra Lawrence-Hardy, Esq., and Jessica Sawyer Wang, Esq., "Are Your Company's Secrets Threatened By Your Employee's MySpace Page?" 28 No. 14 *Andrews Automotive Litig. Rep.* 7 (Jan. 6, 2009).

122 "Submission of MySpace Internet Entry to Newspaper for Publication Does Not Constitute Actionable Invasion of Privacy," 30 No. 6 Cal. Tort Rep. 14 (June 2009).

123 "Facebook: The Future of Service of Process?" 25 No. 8 *Andrews Pharmaceutical Litig. Rep.* 11 (Sept. 21, 2009).

124 "Feds Appeal Dismissal in MySpace Suicide Case," 27 No. 10 *Andrews Computer & Internet Litig. Rep.* 8 (Oct. 14, 2009), citing to *United States v. Drew*, No. 08-CR-00582-UA, 2009 WL 2872855 (C.D. Cal. Aug. 28, 2009).

125 "MySpace is Not Liable for Members' Sexual Assaults," 13 No. 7 *Andrews Telecomm. Indus. Litig. Rep.* 9 (Aug. 19, 2009), citing to *Doe, et al. v. MySpace Inc*., No. B205643, 2009 WL 1862779 (Cal. Ct. App., 2d Dist., Div. 8 June 30, 2009).

126 "MySpace Protective Order Violations," 14 No. 4 Quinlan, *National Bulletin on Domestic Violence Prevention* art. 6 (Apr. 2008).

127 "Second Life Currency Open to Theft," 10 No. 1 *E-Commerce L. Rep.* 12 (Jan. 2008).

128 Nancy McKenna, "Worming its way through Twitter," 5 No. 6 Quinlan, *Computer Crime and Technology in Law Enforcement art.* 5 (June 2009).

129 "Report cites jump in Facebook, Twitter attacks," (Aug. 18, 2009), *Triangle Bus. J.* (Pg. Unavail. Online), 2009 WLNR 16076587.

130 http://www.marketwire.com/press-release/Proofpoint-Inc-1027877.html; "Social networking and reputational risk in the workplace," Deloitte LLP 2009 Ethics & Workplace Survey results.

131 "Social networking and reputational risk in the workplace," Deloitte LLP 2009 Ethics & Workplace Survey results.

132 http://www.marketwire.com/press-release/Proofpoint-Inc-1027877.html

133 http://www.workforce.com/section/02/feature/26/66/08/#

134 Under the recently revised FTC Guides, it is unclear to what extent, if any, an employer may be liable for an employee's statements in social media. Under Example 8 of 16 CFR Part 255.5, An online message board designated for discussions of new music download technology is frequented by MP3 player enthusiasts…. Unbeknownst to the message board community, an employee of a leading playback device manufacturer has been posting messages on the discussion board promoting the manufacturer's product. Knowledge of this poster's employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board. 16 CFR Part 255.1(d) provides that "[a]dvertisers are subject to liability for…failing to disclose material connections between themselves and their endorsers. Endorsers also may be liable for statements made in the course of their endorsements." Therefore, in Example 8, both the employee and the employer may be liable for the employee's failure to disclose his material connection with the employer.

135 16 CFR Part 255.

136 "Facebook, Inc. v. Power Ventures, Inc.," No. C 08-5780, 2009 WL 1299698, at *4 (N.D. Cal. May 11, 2009) ("Access for purposes that explicitly are prohibited by the terms of use is clearly unauthorized.").

137 http://www.myspace.com/index.cfm?fuseaction=misc.terms

138 http://www.facebook.com/terms.php

139 Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e, *et seq.*

140 *See, e.g.,* Cal. Lab. Code § 96k; *see also* N.Y. Labor Code § 201-d.

141 *Laningham v. Carrollton-Farmers Branch Independent School District*, 2009 WL 2998518 (N.D. Tex., Sept. 17, 2009); *Wolfe v. Fayetteville, Arkansas School District*, 600 F.Supp.2d 1011 (W.D. Ark. 2009).

142 National Labor Relations Act, 29 U.S.C. §§ 151-169.

143 Carolyn appreciates the helpful comments of her Insurance Recovery Group colleagues Mark Hersh and Andrew Moss in preparing this chapter.

144 According to a co-national managing director for Professional Risk Solutions at AON, the case of Heartland Payment Systems, a purported breach involving up to 100 million records, led to three sets of claims: consumer class actions for alleged invasion of privacy and potential identity theft; class actions involving financial institutions who had to cancel and re-issue credit cards; and securities class actions alleging that directors and officers did not have adequate oversight measures in place. Phil Gusman "Data Explosion Expands Breach Exposure, But Insureds More Open to Handling Risks," *National Underwriter*, July 20, 2009.

145 *See,* "Cybercrime as A Growth Industry," *Bank Systems + Technology*, Nov. 1, 2009 (available at http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses/13379114-1.html

146 *See,* "A Growing Trend: Social Media As Legal Evidence," *West Michigan Business*, July 29, 2009, available at http://www.mlive.com/business/west-michigan/index.ssf/2009/07/a_growing_trend_social_media_a.html

147 *See,* Phillip K. Anthony and Christine Martin, "Social Media Go to Court," *The National Law Journal*, Feb. 2, 2009; Brad Hamilton, "Inside the YouTube Divorce," *New York Post*, April 20, 2008, at www.nypost.com/seven/04202008/news/nationalnews/inside_youtube_divorce_107240.htm

148 *See,* Andrea Panciera, "Facebook Photo Plays Role in DUI Accident Sentencing," *Providence J.*, May 27, 2008 at http://newsblog.projo.com/2008/05face-book-photo.html; Phillip K. Anthony and Christine Martin, "Social Media Go to Court," *The National Law Journal*, Feb. 2, 2009; See also *United States v. Villanueva*, 2009 WL 455127 (11th Cir. 2009) (affirming district court's sentencing enhancements involving possession of firearm based on statements made in YouTube video and MySpace photos showing defendant with an AK-47 and loaded clip).

149 *See.* John G. Browning, "Dangers of the Online Juror," at http://www.yourhonor.com/IC-Online/IC_Summer09/OnlineDanger2.html

150 *See,* Tom Murse, "Roseboro Juror's Facebook Postings Pose Problems," *Intelligencer Journal Lancaster New Era*, August 4, 2009, available at http://articles.lancasteronline.com/local/4/240616#

151 *See,* John Schwartz, "As Jurors Turn to Web Mistrials Are Popping Up," *The New York Times*, March 17, 2009, available at http://www.nytimes.com/2009/03/18/us/18juries.html

152 *See,* 21 CFR Part 201, *et seq.*

153 There is also the potential that a government regulator will look into whether there has been a violation. In fact, the FDA is so concerned that companies may violate its regulations through social media that it has announced a public hearing Nov. 12-13, 2009, to discuss FDA regulations and social media with a focus on adverse event reporting, levels of disclosure by the company on the information it receives by third parties, and what parameters apply to the posting of "corrective" information about the safety profile of products on company websites. *See,* 74 Fed. Reg. 48083 (Sept. 21, 2009).

154 Examples of how a blog may be used to disseminate information about safety issues related to products are the Consumer Product Safety Commission ("CPSC") blog "on safety," as well as its Twitter page. *See*, http://www.cpsc.gov/onsafety/category/safety-blogs/; http://twitter.com/OnSafety

155 For example, the *New England Journal of Medicine* recently had to issue a statement defending its practices after a survey showed its publication contained more ghostwritten articles than other prominent medical journals. *See* "NEJM responds to survey on ghost-writing," (Sept. 21, 2009); http://www.boston.com/news/health/blog/2009/09/the_new_england.html

156 The learned intermediary doctrine has been adopted in some form in 47 states, with two other states providing supportive language in case law.

157 Furthermore, all electronic communications and advertisements are subject to the retention requirements of the Books and Records Rule.

158 Case No. 09-CV-0128 (S.D. Ind., Sept. 24, 2009).

159 Civil Action No. 08-CV-3859 (JES) (S.D.N.Y. April 24, 2008).

160 Civil Action No. CV09-231, (E.D. Tenn. Aug. 31, 2009).

161 Adam Ostrow, *Twitter Now Growing at a Staggering 1,382 Percent*, MASHABLE THE SOCIAL MEDIA GUIDE (March 16, 2009), *available at* http://mashable.com/2009/03/16/twitter-growth-rate-versus-facebook/

162 *Oneok, Inc. v. Twitter, Inc.*, Case Number 4:09-cv-00597 (N.D. Okl. Sept.r 15, 2009).

163 http://twitter.zendesk.com/forums/26257/entries/18367

164 http://en.wikipedia.org/wiki/Facebook

165 Sally M. Abel, Trademarks and Rights of Publicity in the Converged World, 978 PLI/pat 57, September 2009.

166 http://www.facebook.com/legal/copyright.php?howto_report

167 Allegations of copyright infringement are handled under the directive of the Digital Millennium Copyright Act, a separate form for which is available to users.

168 15 U.S.C. §1114(1)(a).

169 15 U.S.C. §1125(a) liability based on use in commerce of "any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact that is likely to cause confusion."

170 15 U.S.C. §1125(c) liability against party who "at any tome after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark.

171 http://twitter.zendesk.com/forums/26257/entries/18366

172 *Id*.

173 Daniel Boffey, *Trick or Tweet? Twitter Launches Crackdown After Millions are Duped by Fake Accounts*, MAIL ONLINE, September 20, 2009, *available at* http://www.dailymail.co.uk/news/article-1214734/Trick-Tweet-Twitter-launches-crackdown-millions-duped-fake-accounts.html

174 *Anthony La Russa v. Twitter, Inc.*, Case Number CGC-09-488101 (Cal. Super. Ct., San Fran. Co., May 6, 2009).

175 http://twitter.com/help/verified

176 *Taser International Inc. v. Linden Research Inc.*, 2:09-cv-00811 (U.S. D. Ct., D. Ariz., April 17, 2009).

177 http://www.techdirt.com/articles/20090421/1310304599.shtml

178 http://www.bloomberg.com/apps/news?pid=20601103&sid=aR6xHcnBMn9M

179 Nir Kossovsky, MISSION INTANGIBLE, Blog of the Intangible Asset Finance Society, September 21, 2009 (quoting Darren Cohen).

180 *Eros LLC v. Leatherwood*, No. 8:2007cv01158 (M.D. Fla. 2007).

181 *Eros LLC v. Simon*, Case No. 1:2007cv04447 (E.D.N.Y. 2007).

182 Registration No. 3,483,253 covering "providing temporary use of non-downloadable software for animating three-dimensional virtual characters."

183 Registration No. 3,222,158 covering "computer graphics services; graphic art design; graphic design services, graphic illustration serves for others."

184 Registration No. 3,531,683.

185 http://secondlife.com/corporate/tos.php

186 *Id*.

187 *Id*.

188 Abel, *supra* note 138.

189 Kierin Kirby v. Sega of America, Inc., 144 Cal App. 4th 47 (2006).

190 *Marvel v. NCSoft*, No. CV 04-9253 (C.D. Cal. Mar. 9, 2005).

ReedSmith

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
PITTSBURGH
OAKLAND
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE

reedsmith.com

This White Paper is a collaborative effort of the Reed Smith Social Media Task Force, part of Reed Smith's Media & Entertainment Law Practice. It is presented for informational purposes only and is not intended to constitute legal advice.