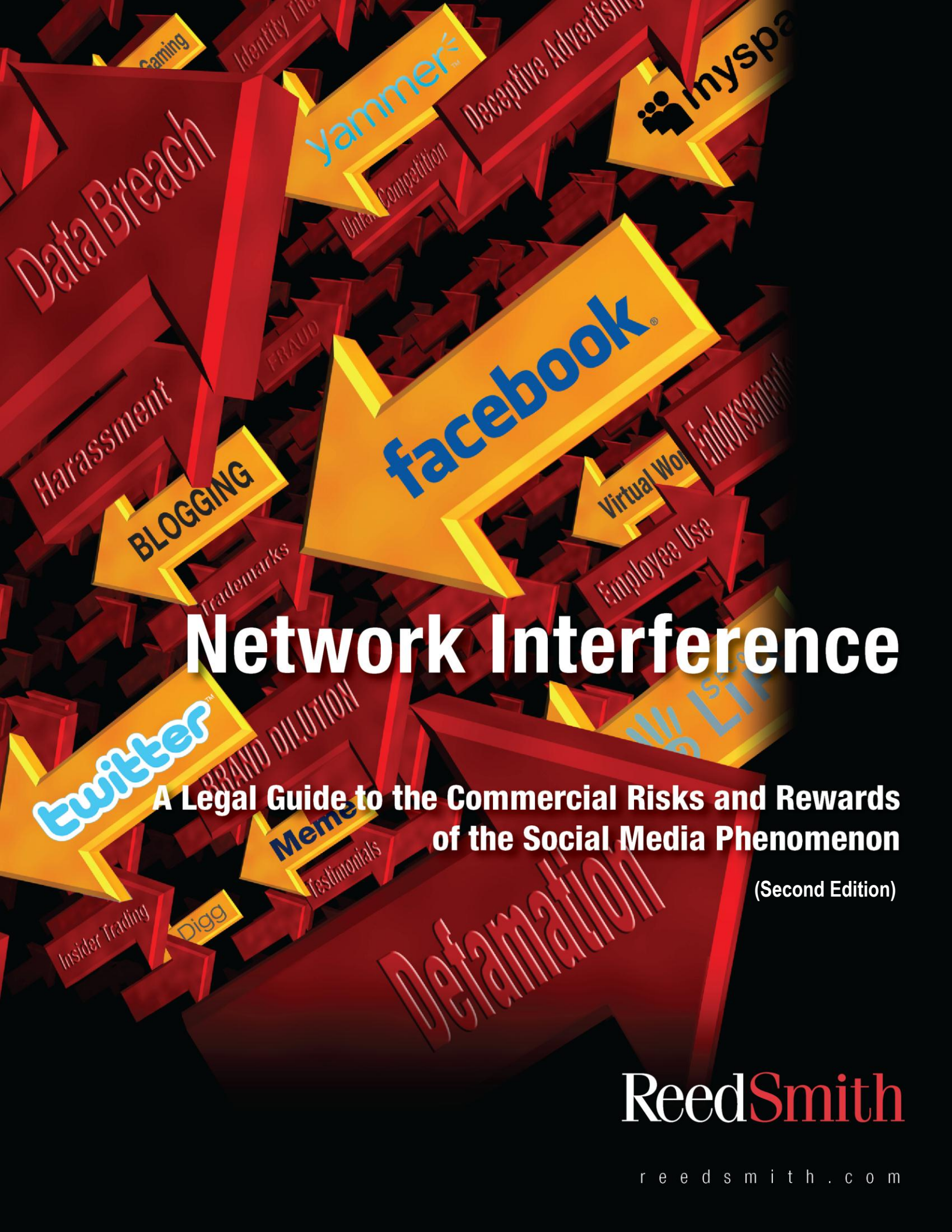


Network Interference

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

(Second Edition)

ReedSmith

reedsmith.com

— PREFACE —

2nd Edition

In October 2009, we published the first edition of this White Paper, focusing primarily on social media issues in the United States. The response was overwhelming and far beyond our expectation—clients, friends, press and social-media communities became engaged with what we had to say. A conversation began that has yet to subside.

The issues we uncovered relating to social media run far deeper than first meets the legal eye. Nonetheless, companies and employees continue to populate social media sites in droves, all too often oblivious to those risks.

But as important as the issues are in the United States, the legal challenges posed by social media know no boundaries. They are truly global. Hence this second edition of the White Paper expanding coverage to Europe. In the future, we'll be expanding further with more editions.

Much has happened in the social media field since the release of the U.S. edition. The CEO of Sun Microsystems resigned on Twitter, and Facebook's privacy settings are now often the subject of front page news. Services like FourSquare are leading the charge into real-time, location-based networking and entertainment, combining the virtual world and the real world. And while the technology advances at an unstoppable rate, the law often lags far behind.

Special thanks also go to the following people, the Social Media Task force members in the United States: Eric Alexander, Sara Begley, Paul Bond, Darren Cohen, Eugene Connors, Colleen Davies, Gerry DiFiore, Michael Golebiewski, Amy Greer, Daniel Herbst, Mark Hersh, Andrew Hurst, Marc Kaufman, Tony Klapper, William Krogh, Kevin Madagan, Stacy Marcus, Mark Melodia, Andrew Moss, Amy Mushahwar, Kathyleen O'Brien, Meredith Pikser, Joe Rosenbaum, Carolyn Rosenberg, Casey Ryan, Nancy Schulein, Sandy Thomas, Lois Thomson. In Europe, thanks go to our members of the Reed Smith Social Media Task Force: Louise Berg, James Boulton, Carl De Cicco, Peter Hardy, Alexander Klett, Emma Lenthall, Paul Llewelyn, Huw Morris, Cynthia O'Donoghue, Stephen Edwards, Laurence G. Rees, Stephan Rippert, Nicolas Sauvage, Katharina Weimer and Michael Young. Contributors are listed alphabetically according to title in each chapter section.

Most importantly, this White Paper remains a living document as we add more chapters and update those we have, making sure it continues to be the definitive source for legal issues in social media. You can access this document by visiting http://www.legalbytes.com/articles/social-and-digital-media-law/.

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.

Gregor Pryor
Editor, Europe

Douglas J. Wood
Editor, United States

— EDITORS —

Gregor Pryor – gpryor@reedsmith.com

Joseph I. Rosenbaum – jrosenbaum@reedsmith.com

Douglas J. Wood – dwood@reedsmith.com

Stacy K. Marcus – smarcus@reedsmith.com

— TABLE OF CONTENTS —

Welcome to the New World

Introduction

Social media is a revolution in the way in which corporations communicate with consumers. This White Paper will help you to maximise the huge potential benefits of this revolution and protect against the inherent legal risks surrounding social media. In this document, you will find practical, action-oriented guidelines as to the state of law in the United States and Europe in the following areas: Advertising & Marketing; Commercial Litigation; Data Privacy & Security; Employment Practices; Food & Drug Administration, Government Contracts & Investigations; Insurance Recovery; Litigation, Evidence & Privilege; Product Liability; Securities; Copyright & Trademarks. As we continue to expand the White Paper, we will add additional chapters as well as updates. So be sure to bookmark http://www.legalbytes.com/ and subscribe to the Legal Bytes blog.

What is Social Media and What Does it Mean to Business?

Everyone has heard of Facebook, YouTube, and MySpace. These are just the tip of the iceberg. There are thousands of social media sites with billions 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. Audiences are not static. 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 memorialised 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]

A Shift in Media Values

Broadcasters have now caught on to the idea that social media fundamentally affects the presentation and even the content of their product. The music industry now embraces social media, using it as a valuable promotional tool. Even the movie industry get in on the act, perhaps even earlier than intended, with the phenomenal success of the online marketing program for the "Blair Witch Project." At the time of its release, the "Blair Witch" site was in the top 50 most-visited sites on the Internet, creating a vibrant "word-of-mouth" campaign that ultimately helped a $750,000 film gross revenues of $250 million. Social media represents a huge opportunity for media and entertainment companies. They can engage with their audience in ways that were previously impossible, and can leverage that engagement with commercial opportunity. However, with this opportunity comes a threat—

YouTube allows everyone to be a broadcaster. As our chapter about copyright demonstrates, social media strikes at the very heart of the proprietorial foundation upon which traditional media campaigns are built.

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 posted 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 after 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 its 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, apologising for what consumers saw and assuring them that such things were neither 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. Doing so while being mindful of the laws that apply in a social media context will help alleviate risk.

What You Need to Do

Every concerned party needs to take some important steps if it 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
- Audit your company's social media programs. Find out what your company and your employees are doing. Do they have any customised 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 cannot 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[13]

United States

Douglas J. Wood, Partner – dwood@reedsmith.com

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

United Kingdom

Huw Morris, Associate – hmorris@reedsmith.com

Germany

Stephan K. Rippert, Partner – srippert@reedsmith.com

Katharina Weimer, Associate – kweimer@reedsmith.com

Introduction

This chapter looks at the relationship between social media and advertising and marketing practices, and how to protect brands.

As an emerging technology with nearly limitless boundaries and possibilities, social media gives consumers unprecedented engagement with a brand. Consumers are empowered. However, this brings with it risks as well as gains. Consumers 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, monetise 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 1.8 billion people use the Internet every day[14], 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 the previous year.[15] The Internet audience is larger than any media audience in history, and it is growing every day. It's those eyeballs that marketers want.

In the UK alone, spending on online advertising grew by almost 5 percent in the first six months of 2009, while television spending fell by 16 percent (*see* IAB UK News, "Internet advertising spend grows by 4.6 per cent"). It was also reported that UK online advertising spend overtook TV advertising spend for the first time.[16] Almost two-thirds of businesses say they intend to spend more on onsite social media, while 64 percent are looking to boost search engine optimisation efforts and 56 percent want to invest more in mobile marketing. Looking forward, new global research by Econsultancy and ExactTarget has revealed that 66 percent of company marketers in the UK intend to spend more on Internet advertising this year compared with 2009. Total Internet advertising spending will surpass £3.5 billion in the UK this year, according to a forecast from eMarketer.

Morgan Stewart, director of research and strategy at ExactTarget, comments: "The shift from offline to online is in full swing as marketers look to measure direct increases in top line sales, site traffic and improve overall marketing return on investment."

In the United States, 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.[17] 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 in September 2009.[18] In February 2010, the COO of Kellogg's confirmed that since 2007, the company had tripled its social media spending.[19] Where are companies spending these dollars? The possibilities are numerous.

National authors begin by examining the use of social media and the risks and gains involved. 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. Some even employ "street teams" of teenagers who plug and promote a brand, movie or music artist in return for relatively small rewards. 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 will discuss its application to the Screen Actors Guild ("SAG") and American Federation of Television and Radio Artists ("AFTRA") commercials contracts.

In our review, we have covered advertising regulation in the United States, the UK and Germany. Note that the UK has a largely self-regulatory environment. This self-regulation comes in the form of codes of practice that are designed to protect consumers and create a level playing field for advertisers. The codes are the responsibility of two industry committees—the Committee of Advertising Practice (CAP) and the Broadcast Committee of Advertising Practice (BCAP), and are independently administered by the Advertising Standards Authority (ASA). Online advertising, including via social networking and the techniques referred to in this chapter, fall under the remit of the CAP Code (which is explained in more detail in Chapter 2).

Social Media in Action in Advertising and Marketing

Brand Awareness

The official Starbucks page has more than 6.8 million fans and counting. The Starbucks YouTube channel has more than 6,000 subscribers and more than 4.5 million upload views of videos. On Flickr, there are two Starbucks groups, each with more than 3,500 members, and a combined total of more than 21,000 photos. And more than 840,000 people are following Starbucks on Twitter. Starbucks' own social network, Starbucks V2V, has nearly 24,000 members.

In this section, we explore the legal issues involved in the use of branded pages and promotions and contests, taking into account the different aspects of U.S., German and UK laws and regulations.

Branded Pages

United States

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 may 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.[20] 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 they provide instructions for submitting a DMCA take-down notice.[21] 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 to 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 nearly 300,000 results, and on MySpace yields more than 91,000 results; and there are more than 3,400 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, organisation, 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 unauthorised 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."[22]

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 parties 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 14 – 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 because of 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.

United Kingdom

As in the United States, advertisers in the UK have embraced viral marketing, advergames, promotions, user-generated content, blogs and brand ambassadors online, as well as exploiting existing social networking sites to grow brand awareness and promote products and services. Social networks offer advertisers reach and engagement of an unprecedented level, combined with clear branding opportunities. However, with that opportunity comes inevitable risk. In-house counsel need to keep abreast of what their businesses are promoting on social media properties to ensure compliance and minimise risk, while maximising the opportunities to reach new audiences and promote the brand.

Later in this chapter, we deal explicitly with the risks associated with corporate blogging and user-generated content, and how companies can take action to help prevent infringement of rights and non-compliance with regulation. In relation to branded pages, our guide for advertisers concerning the addition of terms and conditions for online advertisements (including use and effectiveness of disclaimers and appropriate warnings) is available on the Reed Smith website at www.reedsmith.com. The guide covers issues such as linking to other sites and dealing with difficult users.

Germany

European companies also make use of the possibilities that social networks open up for them. Let's take German car manufacturers as an example. A popular brand owner, BMW, has its own branded page on Facebook and even

localised pages for several countries, including Germany, Indonesia, Mexico and South Africa. The discussion board on the page mainly deals with maintenance and repair issues. However, BMW seems to ignore the questions posted by users and leaves it to other users to respond to these queries. BMW also asks its users to vote on polls and gives them the opportunity to showcase their loved ones. In contrast to BMW's approach, all-time competitor Mercedes Benz does not have a discussion board for users to post their queries, and fans are not allowed to post on Mercedes' wall. It need not be mentioned that apart from the official pages, there are numerous unofficial pages, sub-pages and groups relating to the car manufacturers. As a side note: Porsche tops both BMW and Mercedes regarding the number of fans—it has more than 582,000 fans on Facebook (BMW: 493,000, Mercedes: 241,000). While Porsche, like Mercedes, does not have a discussion page, it allows the users to design their own Porsche and post it to their walls. All of these gimmicks and interactions allow the user to feel close to "their brand," and giving them the opportunity to display their own designed Porsche on their wall is concurrently giving Porsche positive endorsement.

The legal aspects of these brand interactions do not differ materially from the issues raised under U.S. law, as the terms and conditions of the third-party providers like YouTube, Twitter and Facebook are essentially the same. What must be taken into account, though, is that while the European Union has harmonised laws in many areas, including in the area of misleading or false advertising, of commerce on the Internet, and on consumer protection, these laws have been implemented differently in every country. The scope of socially acceptable content may also differ widely within the European Union, given the differences between countries such as Sweden, Bulgaria, the UK, and Spain. Brands that choose to treat Europe as one homogenous state in the course of their social media campaigns run a very real risk of contravening local laws and, possibly just as importantly, offending local sensibilities.

A new phenomenon in the advertising world that reaches the Internet at high speed is so-called "fake advertising." Using the automotive industry again, a video shows a compact car of a German manufacturer driven by a man wearing a traditional Palestinian scarf. He parks the car in front of a street café and activates a belt containing explosives. The guests of the café do not even realise this as no noise or other effect of the explosion reach the outside of the car. The spot finishes with a scroll outlining the model of the car (a Volkswagen) and displaying the slogan "Small but tough." The German car manufacturer had nothing to do with this spot. Virals like this can be very professional in appearance, which makes the determination that it is a fake advertisement difficult. This example triggers various legal questions concerning both the producer of the viral and the company whose products are "advertised." While the advertised company may have claims for trademark infringement, copyright infringement, claims based on unfair competition and even based on tort (passing off and endangering the goodwill of a company) against the producer of the viral, the same company is also at risk of being held liable if the viral infringes third-party rights, and the advertised company had in any way initiated or agreed to the viral (for instance by way of holding a contest for the best video spot involving its compact car and an unsuccessful participant subsequently airs the spot on his Facebook profile). There are many examples of established companies seeking to embrace social media by running user-generated advertising campaigns, only for things to go horribly wrong.

Promotions and Contests

United States

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 10 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 offering contests, giveaways or sweepstakes on Facebook without their prior written consent. Even those who merely use Facebook to publicize a promotion that is otherwise administered and conducted entirely off of Facebook must comply with the Promotions Guidelines. In December 2009, Facebook revised its Promotions Guidelines to specifically require, among other things, that (1) the sponsor take full responsibility for the promotion and follow Facebook's Promotion Guidelines and applicable laws; (2) the promotion is open only to individuals who are at least 18 years of age; (3) the official rules contain an acknowledgement that the promotion is not sponsored, endorsed or administered by, or associated with, Facebook, as well as a complete release for Facebook from each participant; and (4) the sponsor submit all promotion materials to his or her Facebook account representative for review and approval at least seven days prior to the start of the promotion.[23] In addition, Facebook's Promotion Guidelines prohibit, among other things: (1) using Facebook's name in the rules except as otherwise required by the Promotion Guidelines; (2) conditioning entry in the promotion upon a use providing content on Facebook (including, making a post on a profile or Page, status comment or photo upload);

(3) administering a promotion that users automatically enter by becoming a fan of your Page; or (4) administering the promotion on the Facebook site, other than through an application on the Facebook Platform.[24] 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. As a result, several companies have sprung up to assist advertisers in their social media endeavors, including Votigo, Wildfire and Strutta, just to name a few. One such company is Folgers. Folgers recently launched a social media contest to celebrate the 25th anniversary of its famous Folgers jingle, "The Best Part of Wakin' Up." The contest, located at a dedicated URL, encourages people to submit their take on the iconic jingle (*See "User-Generated Content" below for issues relating to UGC.*) Entrants have a chance to win $25,000 and potentially have their jingle featured in a future Folgers Coffee commercial. In addition to the Grand Prize awarded for the jingle itself, daily prizes and a grand prize will be awarded via random drawings to individuals who submit votes in the jingle contest. It doesn't take much imagination to come up with the legal issues and challenges—consumer, talent union and regulatory—that might be raised. What if the winner is a member of a union? Who owns the video submissions? Will the semi-finalists, finalists and/or winners be required to enter into a separate agreement relating to ownership of the master recording?

Despite the undeniable reach of social media, participation is not always easy to come by. Just ask FunJet Vacations. In fall 2009, FunJet sponsored a giveaway whereby individuals who uploaded a photo or video of themselves making a snow angel were entered in a drawing for a four-night vacation in the Mexico or Caribbean. Seems like an easy sell, especially given the winter we had here in the Northeast, right? Wrong. According to Mike Kornacki, who assisted Funjet Vacations in the giveaway, "on the 1st level market reach Funjet was at 384,000 individuals for Facebook and 1.05 million for Twitter" and Funjet only received "313 total submissions over 5 days."[25] So what happened? Those who did participate were unwilling to share the giveaway with their networks because "they didn't want the competition."[26] Individuals Mr. Kornacki surveyed who didn't participate said "it was too hard to enter the drawing." Seriously? Taking a photo of yourself making a snow angel and uploading it to a micro-site is too hard? Those individuals must find Flickr, YouTube and Shutterfly simply unbearable.

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[27], 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[28]). 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.[29] 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.[30]

Germany

As already highlighted earlier in this chapter, companies that wish to conduct promotions, sweepstakes, raffles and similar activities in Europe need to be aware that while there is certainly European harmonised law, the Member States may have implemented the Directives differently. Certain jurisdictions like France are known for adding little tweaks and adopting a very restrictive and consumer-protective approach to advertising. While the above-mentioned golden rule of "no purchase necessary to enter or to win" provides minimum guidance for contests in Europe, companies should nevertheless obtain local clearance advice. Various provisions in local law make the running of promotions on a European-wide basis a challenge. Italy, for instance, requires that if the raffle or contest is actively promoted in Italy, the organising company must have someone on the ground in Italy to conduct it. This gives rise to a flourishing business segment of promotion agencies. A company that advertises a promotion via a social network should not fall prey to the assumption that because the promotion is run from a ".com" homepage it is subject to U.S. law only, or that it

could adopt the law of a particular country while excluding all other jurisdictions. As soon as a promotion is aimed at the citizens of a European country, that country is likely to assume jurisdiction and deem its laws applicable to the promotion.

Brand Interaction

Bloggers

United States

"People are either going to talk with you or about you."[31] 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 (hoped-for favourable) 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 criticised 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. In 2009, the Federal Trade Commission ("FTC") revised its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* (the "FTC Guides")[32]. 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."[33]

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.

United Kingdom

Applying the principles described above in relation to the United States helps identify, from the perspective of English law and regulation, the main risks associated with external corporate blogging and participating in social networking sites:

- Damage to reputation: This typically arises if a blogger says something that may tarnish the reputation of the company in the eyes of other readers. It could be an innocent criticism of the product or company or a more deliberate campaign.
- Breaching advertising regulations: This can cause damage to brand reputation, particularly where the breach leads to advertising regulators publishing adverse adjudications about the owner of the brand
- Liability for infringement of intellectual property rights: The biggest risk here is that a participant or blogger copies content for the blog post from another source without permission. Music is particularly risky, but any image, text or creative material may have been sourced from a third party without their knowledge.
- Liability for defamation or illegal content: Defamation is perhaps one of the greatest risks, especially if blog

participants are given a free reign. See our later chapter concerning defamation.

- Breaching data protection laws and/or invading privacy: See our later chapter for more details concerning these risks.
- Leaking confidential information: Often risks emanate not from external sources but from employees within the company engaging in blogging. Details of a new product launch or disclosure of poor financial figures can innocently be disclosed if safeguards are not put in place. This can cause damage to the business and, potentially, breach of corporate securities rules.

Germany

Advertisement in blogs is also increasingly happening in Europe, but the European Commission has not initiated legislative action yet. A prominent example for using blogs for advertisement was constituted by the Coty Prestige Lancaster Group. The company decided to launch a teaser campaign prior to the traditional campaign for the perfume ck-IN2U. They created rather attractive and sexy fake identities in various blogs and used them to tease the blogosphere about the perfume. And at the end of each post, they added the sentence "what are you in2?" After being found out, Coty Prestige Lancaster Group quickly stopped the campaign. While many bloggers perceived this behaviour as contravening an unwritten blogger's code of ethics (and indeed blog operators are looking for ways of prohibiting unwanted advertising activities in their blogs), the more crucial question is whether the multiple five-digit-claims that the responsible advertising agency has received will hold up. Under German law, for example, the agency may be obligated, pursuant to the legal institute of "agency by necessity,", to pay to the blog operators the amount saved by avoiding the traditional booking of advertising space on the blog or surrounding the blog. Comparable decisions have been made with regard to the unauthorised use of photographs. However, court decisions on advertisement in blogs have not reached the press…yet.

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[34] and the Lab[35]. 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 utilised to discuss other important issues facing the company."[36] The Lab is "a pilot program for GM, an interactive design research community in the making."[37] 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."[38] 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."[39]

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 services 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 6 – 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? More perniciously, was it a competitor? 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 authorised 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

United States

UGC covers a broad spectrum of content, from forum postings, to photos to audiovisual 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 contests that are set up as a comparison of one brand to another, things can get dicey.

Following the court's denial of its motion for summary judgment, on February 23, 2010, Quiznos settled its nearly three-year-old dispute with Subway stemming from the "Quiznos v. Subways Ad Challenge." The Challenge solicited videos from users depicting that Quiznos' sandwiches have more meat than Subway's sandwiches. In 2007, Subway filed a lawsuit against Quiznos[40] claiming that by airing the winning video from the Quiznos contest, Quiznos had engaged in false and misleading advertising under the Lanham Act. In denying Quiznos' motion for summary judgment, the court found that Quiznos was a provider of an interactive computer service, but declined to decide whether the UGC videos at issue were "provided" by Quiznos or by a third party (a requirement for CDA immunity). The court determined that it was a question of fact as to whether Quiznos was actively responsible for the creation of the UGC.[41]

Following the court's decision in the Quiznos/Subway case, the question that remains is: how much control is too much? At what point, is a sponsor of a UGC promotion "actively responsible" for the UGC?

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.

United Kingdom

A question that arises often where a company includes social media elements or features on its own properties, or in advertising or promotional campaigns, is whether those elements or features should be moderated.

A conservative and perhaps safer approach is for brands to moderate sites for unwelcome content or comments. Moderation can take several forms: (i) pre-moderation; (ii) post-moderation; and (iii) reactive moderation. The fact that moderation affords control to the brand owner and helps them limit any potentially risky business means that brand owners often favour a pro-moderation approach. However, moderation itself can be a risky business and can sometimes be one that advertisers and their advertising agencies or others ought not to do themselves.

By checking all material prior to publication, the operator of a site could be said to assume responsibility for the material that appears. This makes pre-moderation a relatively high-risk and labour-intensive approach. However, many brand owners feel uncomfortable about not moderating, and the decision may well come down to the sort of site in question. For example, we recommend that any site used by children ought to be properly moderated by specialists who are also provided with guidelines on how to carry out their role. Equally, sites that carry less risk may be better suited to a post-moderation or even reactive moderation approach, whereby moderation only takes place in response to feedback from users.

We recommend that moderation, and whether to take responsibility for moderation, be considered carefully, taking into account the nature of the product or service in question and the potential propensity for damage to the brand. In some circumstances, it may be appropriate to outsource moderation activity to a specialist company that can shoulder the administrative burden. In addition, sites that carry user-generated content should include terms of use with appropriate warranties. Finally, brands may wish to seek insurance for liability created by user-generated content.

Where advertisers are considering using third-party sites for advertising purposes (for example, Facebook), they may also consider whether or not to moderate the areas of the site that are within the control of the advertiser.

The alternative to a moderated environment is for a brand or agency to allow the site or property to operate without moderation. There are many downsides to this approach. For example, when content is unmoderated, the quality of material posted is difficult to control. There is, on the face of it, a legal advantage to unmoderated sites, in that a brand or site operator can more easily seek an exemption from liability for anything that is defamatory, infringing or otherwise unlawful. This exemption is afforded by local laws deriving from the E-Commerce Directive, as discussed in later chapters, and the only material condition

of the exemption is that the operator of the site provides a process for removing offending content expeditiously upon being made aware of it. However, guidance from UK government agencies counsels against unmoderated environments generally.

In the case of either moderated or unmoderated sites, it is essential that the process for the removal of content is easy, and that concerned individual users can report inappropriate content to the operator swiftly. The operator must then be able to deal with the complaint or problem and have clear guidelines for doing so. It is recommended that operators provide a link on each page of the website that clearly directs users to the process for reporting inappropriate content. Phrases such as "Report Abuse," "Complain about this content" or "Flag as inappropriate" are all commonly used as links. The operator of a site should also require clarity in a complaint and seek to ensure the user is required to explain exactly why a complaint is being made, so as to enable the assessment of the merits of any objection.

Germany

The laws in Europe concerning liability for UGC are similar to those in the United States in some respects, but in other areas are markedly different. Importantly, the laws in Europe are developing quickly in this area and are, some might say, becoming more conservative and in favour of rights holders than in the United States.

The European Union regulated certain aspects of electronic commerce in its Directive 2000/31/EC ("Directive"). The Directive was introduced to clarify and harmonise the rules of online business throughout Europe, with the aim of boosting consumer confidence. It also seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States. The Directive applies to the Member States of the European Economic Area (''EEA''), which includes the 25 Member States of the EU plus Norway, Iceland and Liechtenstein.

The Directive contains specific provisions on liability for hosting services. The general principle is that a service provider shall not be liable for the information stored if the provider does not have actual knowledge of illegal activity or information, and where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful. If the service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, there is no liability. Hence the service provider must act immediately upon gaining knowledge that the material is unlawful by either removing or disabling access to the material.

The Directive further makes clear that a service provider has no obligation to monitor the content. The Directive states that Member States must not impose a general obligation on service providers to monitor the information that they transmit or store. A service provider can make use of the aforementioned limitations in liability as long as it is clear that the content is content from someone else, *i.e.* UGC. Hence in case of UGC advertisements or uploads, the service provider has to avoid assuming such UGC as its own content to avoid liability in connection with such content. The critical question for companies using UGC arises when the company assumes UGC as its own content. It is likely that UGC will be considered as a company's content if it is made as part of the company's own offering. A recent decision of the German Supreme Court[42] illustrates the thin line between third-party content and own content. In the case, the defendant offered free cooking recipes on its website www.chefkoch.de. Every user can upload its own recipes with pictures on that website. One user uploaded a picture from a different cookbook website – the plaintiff's. The Supreme Court considered the defendant liable as publisher of the picture by placing its logo on each uploaded recipe, among other things. The defendant hence should have checked the legality of each picture that was uploaded by users. In practice, this may be an impossible task. Many companies that attempt to ''clear'' user-uploaded content before publication find that the majority of submissions are unusable.

Even if a company does not assume responsibility for third-party content, it is crucial that terms and conditions set forth clear rules regarding UGC.

The Bottom Line: You need to have specific Terms and Conditions in place regarding content uploaded by users. Those terms and conditions should specify that such content does not violate any third-party rights, including moral rights and copyrights, and does not contain any defamatory, libelous, racial, pornographic content. You should indicate UGC as such. You should not use UGC for your own offering or otherwise you might assume liability for its content. You need to observe the notice and take-down principle. In case specific illegal content will be repeatedly uploaded, you need to take measures to prevent such continuous infringement, *i.e.*, terminate user access, or install certain filter software. You must not automatically assume that you will be protected by safe harbour defences.

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").[43] 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 unauthorised exhibition of a commercial, nor is that advertiser responsible for policing such unauthorised 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

United States

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 14 – Trademarks*), the DMCA, the CDA (*See Chapter 2 – Commercial Litigation*), CAN-SPAM and state unfair trade practice acts.

Europe

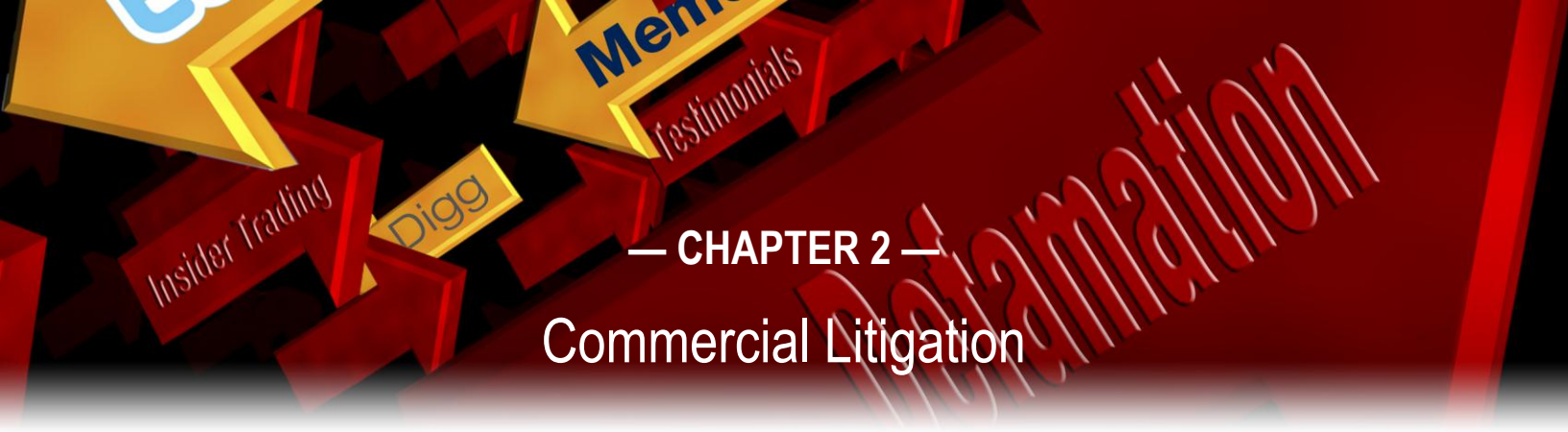
The Directive 2006/114/EC dated 12 December 2006 regulates misleading and comparative advertising; the Directive 2005/29/EU dated 11 May 2005 regulates unfair business-to-consumer commercial practices.

In addition, there are numerous self-regulatory regimes and organisations dealing with advertising regulation. These national bodies cannot be ignored. On a European level, the European Advertising Standards Alliance ("EASA") acts as the chief self-regulator. EASA is based in Brussels and is a European voice of the advertising industry. It acts as the European coordination point for advertising self-regulatory bodies and systems across Europe.

Bottom Line—What You Need to Do

Social media implications and applications to advertising and marketing cannot be ignored. While active or passive participation can enhance and promote brand presence, a danger of brand damage also always exists, and risks should be minimized by prudent planning. 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.

Companies operating campaigns in numerous jurisdictions, even across Europe, cannot take a one-size-fits-all approach to compliance with advertising laws and regulation. By its nature, social media has additional pitfalls for advertisers. A non-compliant or culturally insensitive message on a social media destination can cause significant harm to a brand.



— CHAPTER 2 —

Commercial Litigation

Chapter Authors

United States

John L. Hines, Jr., Partner

Janice D. Kubow, Associate

United Kingdom

Emma Lenthall, Partner – elenthall@reedsmith.com

Louise Berg, Associate – lberg@reedsmith.com

Introduction

This chapter explores emerging exposures associated with misleading 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, misleading advertising and defamation. Within the realm of misleading 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 US position

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.[44] 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.[45]

False Advertising Generally

Generally, the tapestry of laws covering false advertising consists of Section 5 of the FTC Act[46] (the "FTC Act"), Section 43(a) of the Lanham Act,[47] 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."[48] According to the FTC Policy Statement on Deception (1983),[49] 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.[50] 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.[51] The advertiser generally bears the burden of substantiating the advertising claim.[52] The FTC Act permits monetary and injunctive relief.[53]

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.[54] 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.[55] 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.[56] 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.[57] 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.[58]

"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."[59]

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.[60] 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." 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?"[61]

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.[62] 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.[63] 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)*:[64]

> 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."[65] 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."[66] 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."[67] 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."[68]

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."[69] 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."[70] To avoid prosecution, if not liability, advertisers should heed the Commission's admonition:[71]

> [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:[72]

> 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 recognises 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.[73]

In *Doe v. Friendfinder Network, Inc.*,[74] 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:[75]

> 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."

The UK position

While there is at present no specific legislation aimed at social media, there is a plethora of legislation and self-regulation that impacts on almost all activities connected to blogging, social networking or undertaking new forms of promotions on line. Some of the most important legal controls are:

The Advertising Standards Authority and the 'CAP' Code

The Advertising Standards Authority is an independent body which regulates all forms of advertising, sales promotion and direct marketing in the UK. Different regimes apply to broadcast and non-broadcast advertising. Online advertisements are covered by the self regulatory 'non-broadcast' Codes of Advertising Practice (CAP Code). [76]. While this Code only applies at present to advertisements in 'paid for' space, this is likely to change shortly. There is huge political pressure to extend the remit of the ASA and the CAP Code to all promotional messages on the Internet. In any event, all sales promotions are covered by the CAP Code. Advertisers need to be aware of the need for compliance with the Code. For example, the ASA regulates pop-up and banner ads on social networking sites and viral email or other marketing messages which advertisers pay social media to seed, though the position is not entirely clear. In addition there is a risk that Trading Standards or other regulators could intervene by utilising legislation, as described further below.

The ASA will not regulate any advertisements published in foreign media or which originate from outside the UK. Advertisers need only be concerned if they are placing an advertisement on a UK-based social networking site. However, the ASA does operate a cross-border complaints system in conjunction with 'EASA', the European Advertising Standards Alliance.

The CAP Code sets out a number of key principles to protect consumers against false advertising and other harmful advertising practices. For example, it states that advertising should be legal, decent, honest and truthful, and should not mislead by inaccuracy, ambiguity, exaggeration or otherwise), should not cause offence and should not contain misleading comparisons. It also contains specific rules relating to particular types of advertisement and products.

The UK non-broadcast advertising industry is self-regulating and therefore compliance with the CAP Code is voluntary. However, penalties for breaching the Code can include the following.

- *Refusal of further advertising space:* The ASA can ask sellers of ad space in all media to refuse to carry an ad
- *Adverse publicity:* ASA adjudications are published weekly and can be widely reported by the media
- Withdrawal of certain trading privileges (*e.g.*, discounts)
- Enforced pre-publication vetting
- Ineligibility for industry awards
- Legal proceedings: In the case of misleading ads or ads which contain unfair comparisons, the ASA can refer the matter to the Office of Fair Trading. The OFT can seek undertakings or an injunction through the courts or issue an Enforcement Order under the Enterprise Act 2002.

Advertisers also need to be aware that more powerful sanctions are in the pipeline and that, practically speaking, the risk of damage to the brand by an adverse adjudication is a real deterrent to most reputable advertisers and brand owners.

Advertisers who like to put out edgy content do not necessarily need to fear ASA regulation. ASA adjudications do not automatically stamp out anything which pushes the boundaries. As an example, a company called Holidayextras paid video site Kontraband to carry a viral ad for internet parking. The ad featured a man speaking with a heavy Irish accent who was running a dodgy car parking operation. He stumbled out of a caravan (beside which were a fence and a sign saying 'ca parkin') and swore as he chased off children and threw a chair at them. Throughout the ad, subtitles appeared which were a more polite interpretation of his words (for example, he appeared to kick a car and punch the driver and the subtitles stated "Just pop it in the space over there please Parker"; "There's a good chap"). More extreme behaviour and questionable practices followed, and at the end of the ad, a car was shown on fire. From his caravan the man phoned the customer saying "there's been a slight problem with

your Mondeo". The ASA failed to uphold a complaint that the ad was offensive to Irish people and Romany travellers. They noted the ad was intended to show a humorous contrast between a fictional caricature and a company that valued security. Although the character spoke with a heavy Irish accent and ran his business from a caravan, because he displayed extreme behaviour from which the humour in the ad was derived, they did not consider the ad suggested that behaviour was typical of Irish or Romany communities. Whilst they understood that some people could find the ad in poor taste they concluded it was unlikely to cause serious or widespread offence.

False Endorsements

It is unlikely that the ASA will regulate third party endorsements of an advertisers' products which appear on social media, unless the advertisers paid or actively participated with the media provider to put them there. As noted above, only ads in 'paid-for' space fall within the ASA's remit, subject to possible imminent change as mentioned above.

However, advertisers who place 'paid for' ads containing endorsements should be aware that, according to the CAP Code, they should obtain written permission before referring to/portraying members of the public or their identifiable possessions, referring to people with a public profile or implying any personal approval of the advertised products. They should also hold signed and dated proof (including a contact address) for any testimonial they use. Unless they are genuine opinions from a published source, testimonials should be used only with the written permission of those giving them.

Advertisers should take particular care when falsely representing that a celebrity has endorsed their products or services as they could be vulnerable to a claim for passing off (regardless of whether the endorsement appears in paid-for space). Unlike most other jurisdictions, it is possible under English law to use dead and living celebrities without consent, provided there is no implied endorsement or a breach of any trade mark. The danger with the Internet, however, is that material may be accessible in jurisdictions outside the UK and therefore using the image of celebrities without permission in the online environment carries a greater degree of risk than on more traditional media.

Passing Off

Passing off is a cause of action under English common law. It occurs where consumers are misled by someone who is making use of another person's reputation, and can take two forms:

- direct passing off, where an individual falsely states that his goods or services are those of someone else (for example, if someone were to set up a fake YouTube site);
- indirect passing off, where someone is promoting or presenting a product or service as impliedly associated with, or approved by someone else when that is not the case (for example, where an advertiser produces a fake viral which appears to show a celebrity using their product. Liability could result even if lookalikes or soundalikes are used).

Consumer Protection from Unfair Trading Regulations 2008

False advertising and word-of mouth marketing on social media could also fall foul of the Consumer Protection from Unfair Trading Regulations 2008 (which implement the EU Unfair Commercial Practices Directive in the UK). The regulations include a general prohibition on unfair business to consumer commercial practices which is so wide that its application could extend to a variety of commercial practices on social media. The regulations also legislate against misleading actions/omissions and aggressive commercial practices, and set out prohibitions on 31 specific practices that will be deemed unfair in any circumstances. Several of these could be relevant to commercial activity on social media. As an example, prohibition 11 prevents traders from using editorial content in the media to promote their products or services without making it clear that the promotion has been paid for. The prohibitions apply to any 'trader', *i.e.*, a natural or legal person acting in the course of his trade, business, craft or profession. Contravention can lead to criminal penalties. This does not bode well for so-called 'street teams' as used by some brands to promote products. Street teams are often young people who are employed on a part-time basis to eulogise about a particular brand or product on social media platforms. Often difficult to spot, street teams can be hugely effective at driving brand equity because consumers do not realise that they are being targeted – instead, they believe that they are truly on the receiving end of genuine word-of-mouth recommendations.

Advertisers may also find useful the Word of Mouth Association UK Code of Ethics useful see http://womuk.net/ethics/. The Word of Mouth Marketing Association ("WOMMA") and WOM UK are the official trade associations that represent the interests of the word of mouth and social media industry. The Code sets standards

of conduct required for members that include sensible guidelines on the disclosure of commercial interests behind on line commercial activities and social network sites.

The Business Protection from Misleading Marketing Regulations 2008

The Business Protection from Misleading Marketing Regulations 2008 prohibit misleading advertising and set out rules for comparative advertising. Advertising is defined as 'any form of representation which is made in connection with a trade, business, craft or profession in order to promote the supply or transfer of a product'. This broad definition could clearly cover false advertising and word-of–mouth marketing (as well as other content) on social media. A trader who falls foul of the regulations can be punished by a fine (or imprisonment for engaging in misleading advertising). A trader is defined as any person who is acting for purposes relating to his trade, craft, business or profession and anyone acting on their behalf. There is a defence for the 'innocent' publication of advertisements.

Social networking: a new form of advertising regulation?

The most effective means of controlling advertiser activity in the modern world is the ability for consumers to voice their discontent.

Sometimes social networking sites may enable consumers to send a message to advertisers where the regulator can't. In January 2010, more than a thousand people joined a Facebook campaign to ban UK billboard advertising a website for those looking for "extramarital relations". The ASA had rejected a complaint about the billboard on the grounds that the ad would not cause "serious or widespread offence" and said that its remit was to examine the ad in isolation, rather than the product it was promoting, which is a legally available service. At the time of writing, the group had over 2,700 members

> Equally the damage that can occur when a brand misleads the public can much more easily be broadcast to a wider audience via social networking and blogging sites.

Defamation and Harmful Speech: Managing Corporate Reputations

The U.S. position

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."[77] 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."[78]

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.[79] 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.[80] 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.[81] 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."[82] 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."[83] 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.*,[84] 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.[85] The Texas District Court rejected the claim, and in doing so highlighted the potential breadth of the "immunity":[86]

> 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.[87] 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.[88]

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.[89] 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)."[90] It is worth emphasizing that the Section 230 bar applies to providers "or users" of interactive computer services.[91] Significantly, there is at least an argument that re-tweeters (as "users") are protected under the statute.

Plaintiffs continue to reach for creative attacks on Section 230. In *Finkel v. Facebook, Inc., et al.*,[92] 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."[93] 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."[94] 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.*,[95] 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."[96]

This result is consistent with the Ninth Circuit's decision in *Fair Housing Council of San Diego v. Roommates.com, LLC*.[97] 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.[98] 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.[99]

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."[100] 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.[101]

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*,[102] 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.'"[103] 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.[104]

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.[105] Courts continue to consider similar issues, and a number of legislative proposals have been introduced at the state and federal level.

Most recently, the New Jersey appellate court considered the issue in *Too Much Media, LLC v. Hale*,[106] where the court offered useful guidance on attributes distinguishing providers of information that are "news media" (and giving rise to a reporter's privilege) and those that are not. In that case, a software provider in the adult entertainment sector brought a defamation claim against the defendant who operated a blog targeting pornography. The New Jersey court rejected the defendant's assertion of the reporter's privilege in response to plaintiff's discovery for information relating to sources of certain information posted on the blog. Among other factors, the court noted that the defendant "produced no credentials or proof of affiliation with any recognized news entity, nor has she demonstrated adherence to any standard of professional responsibility regulating institutional journalism, such as editing, fact-checking or disclosure of conflicts of interest."[107] The court went on to note "[a]t best, the evidence reveals defendant was merely assembling the writings and postings of others. She created no independent product of her own nor made a material substantive contribution to the work of others."[108]

Ratings Sites

Social media has given rise to a proliferation of ratings sites. Many businesses are beginning to feel the effects of online negative reviews. The ratings sites themselves, however, need to tread carefully because the negatively affected businesses are jumping at the chance to shift their losses back to the ratings site.

Traditionally, ratings sites have two primary defenses.

First, to the extent that site operator itself is rating sites, the site operator's system and/or list may be protected under the First Amendment as its "opinion." Second to the extent

that the site is carrying the ratings of third parties, the ratings site operator is protected under Section 230 of the Communications Decency Act for the tortious speech of the third parties who blog their ratings on the site (*e.g.*, defamatory ratings).

The cases supporting an opinion defense reach back to cases challenging securities and credit ratings, such as *Jefferson County Sch. Dist. No. R-1 v. Moody's Inv. Services, Inc.*[109] In *Search King Inc. v. Google, Inc. v. Google Technology, Inc.*,[110] which relied on *Jefferson County Sch. Dist.*, Search King allegedly promoted an advertising business that identified highly ranked sites and then worked out deals with those sites to sell advertising on behalf of other companies. Google allegedly disapproved of Search King's business model (which capitalized on Google's PageRank ranking system) and responded by moving Search King itself to a lower page rank—causing it to move off the first page for certain queries. Rejecting Search King's claim for interference with business advantage on the grounds that Google's PageRank algorithm is protected opinion, the court found that manipulating the results of PageRank were not actionable because there was "no conceivable way to prove that the relative significance assigned to a given web site is false."

Cases involving credit and securities ratings continue to be worth monitoring as relevant precedent for Internet ratings cases. In one of the cases growing out of the recent sub-prime crisis against Moody's, Standard and Poor's and other securities ratings agencies, a New York federal court rejected "the arguments that the Ratings Agencies' ratings in this case are nonactionable opinions. 'An opinion may still be actionable if the speaker does not genuinely and reasonably believe it or if it is without basis in fact.'"[111] Rejecting the argument that Jefferson County Sch. Dist. mandated a different result, the court noted that even under that case "'[i]f such an opinion were shown to have materially false components, the issuer should not be shielded from liability by raising the word 'opinion' as a shibboleth.'"[112]

In the context of Internet ratings sites, it remains to be seen just where courts draw the line at such material false components, but ratings companies are obviously well advised to tailor their public statements and documents very precisely to their actual practices.

Ratings sites will have to be careful about not taking action that causes them to lose their immunity under Section 230. As an example of the kinds of cases to watch for, Yelp was recently sued in various class actions for allegedly manipulating the appearance of consumer reviews in instances in which the site reviewed had not purchased advertising from Yelp.[113] Yelp purports to help people find the "right" local business by listing consumer reviews; in order to correct for unduly malicious or biased reviews, all reviews are filtered through Yelp's algorithm. Plaintiffs have claimed that Yelp circumvented the algorithm—suppressing positive reviews and emphasizing negative ones—in cases in which the reviewed site refused to buy advertising. Yelp has vigorously denied the allegations and is also waging a thoughtful collateral campaign through social media (including a YouTube video on how its filtering works).

These claims are demonstrative of the kinds of claims ratings sites are likely to face. If this kind of conduct was in fact endemic to the site, the plaintiffs would have a basis to argue against Section 230 immunity generally.

Defamation Law in England

The UK position

Generally speaking, the English courts are less vigorous in their defence of free speech than their American counterparts. There is no equivalent to the First Amendment in England. The outcome of a defamation case is decided by balancing the right to free speech against the right to reputation. Under the European Convention of Human Rights (which has been enacted into UK law) these rights are of equal value.

As a result of the greater protection given to reputation in comparison with other jurisdictions (such as the United States), the UK has become the forum of choice for many defamation claimants.

To prove defamation under English law, the claimant must show that a statement:

- is defamatory (*i.e.*, is a statement which tends to lower the claimant in the estimation of right-thinking members of society generally);
- identifies or refers to the claimant; and
- is published by the defendant to a third party.

A number of claims have already been made under UK defamation law in respect of social networking sites. In *Applause Store Productions and Firsht v Raphael (2008)*, the defendant, a former friend of Matthew Firsht, set up a Facebook profile in Firsht's name and a Facebook group entitled 'Has Matthew Firsht lied to you?'. This contained defamatory material suggesting that he and his company had lied to avoid paying debts. This was found to be

libelous and damages of £22,000 were awarded. The judge took into account the likelihood of a high level of hits on the webpage – here it could be accessed by the Facebook London group which had around 850,000 members.

The rise of social media has resulted in a prevalence of 'hate' sites – blogs or Facebook groups specifically set up to promote the 'hatred' of a celebrity or a company. There is therefore plenty of scope for defamation claims, but statements on these sites will not always be defamatory. In *Sheffield Wednesday Football Club Limited v Neil Hargreaves (2007)* which concerned postings on a football club fan website about the club's management, the judge considered whether the statements could "reasonably be understood to allege greed, selfishness, untrustworthiness and dishonest behaviour" and were therefore defamatory, or whether the posts were mere "saloon-bar moanings".

One key difference between US defamation law is that the UK does not have the single publication rule – so on the internet, a new cause of action arises every time the website is accessed. This has been criticised as online publishers potentially face unlimited liability in respect of older material which remains on their sites. The government launched a consultation in September 2009 to consider changing this in relation to online publications.

Anonymous Speech

A Norwich Pharmacal order is an order which the UK courts may make requiring a third party to disclose information to a claimant or potential claimant in a legal action. Where a third party is involved in the wrongful acts of others (whether innocently or not), they have a duty to assist the party injured by those acts, and so a court will order them to reveal relevant information.

Norwich Pharmacal orders can be used to require social networking sites to disclose the identities of site users. For example, in the Sheffield Wednesday case referred to above, the High Court ordered the operator of the football club fan website to disclose the identifies of four users of the site who had posted the allegedly defamatory messages concerning the club's management. A similar order was obtained against Facebook in the Applause Store case referred to above.

Service Provider Immunity

EC Directive 2000/31/EC (the E-commerce Directive) states that Internet service providers ("ISPs") providing hosting services receive partial immunity from defamation (and other) actions (Article 14). An ISP will be immune if it does not have actual knowledge of illegal activity or information, or knowledge of the facts or circumstances from which it is apparent that the activity or information is illegal.

An ISP will lose immunity if, on obtaining knowledge of the illegal activity, it fails to act expeditiously to remove or to disable access to the information.

Section 1 of the English Defamation Act 1996 provides a similar defence where a secondary publisher takes reasonable care in relation to the publication of the statement, and did not know and had no reason to believe that what he did caused or contributed to the publication of a defamatory statement.

As a result of these provisions and cases which interpret them, ISP immunity in the UK is much narrower than in the United States. ISPs can lose their immunity if they know or ought to know about infringing statements and are therefore more likely to take action to remove possibly defamatory statements.

In *Godfrey v Demon Internet Limited* (1999, pre-dating the E-Commerce Directive) a defamatory statement was posted on a Usenet newsgroup and the ISP was named as a defendant. The claimant sent the ISP a fax informing it of the defamatory statement and requesting its removal. The defendant ignored this and allowed the statement to remain for a further 10 days. It was held that the ISP was a common law publisher of the material and as it knew of the offending statement but chose not to remove it, it placed itself in an 'insuperable difficulty' and could not benefit from the s1 defence in the Defamation Act.

However, an ISP who does not host the information or have an involvement in initiating, selecting or modifying the material, and effectively acts only as a conduit, will have a defence under the Defamation Act and the E-Commerce Regulations. This was demonstrated in the case of *Bunt v Tilley (2006)*, where a number of ISPs were absolved from liability in respect of defamatory postings on newsgroups.

It is in an ISP's interests to be quick to remove defamatory material if they wish to remain immune. For example, after the Godfrey case above, the ISP removed the comments and suspended newsgroup access to certain members until they signed a form of indemnity. Similarly, another ISP, Kingston Internet Limited, shut down an 'anti-judge website' after the Lord Chancellor's department wrote to complain. However, by requiring ISPs to act in this way, it could be argued that the law goes beyond what is necessary, and that the scales are being pushed too far in favour of protection of reputation at the expense of free speech.

Protection of Sources

Like the U.S., the UK has laws which protect journalistic sources. However, unlike the U.S., protection is not afforded only to newspapers. The relevant provision (section 10 of the Contempt of Court Act 1981) states that 'no court may require a person to disclose, nor is any person guilty of contempt of court for failing to disclose, the source of a publication for which he is responsible, unless it is established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security, or for the prevention of disorder or crime'. This wording clearly extends beyond journalists and could apply to social media. However, as the public policy reasoning behind the section may not be there in the case of many publications on social media, a court may be more ready to find that disclosure is necessary.

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 optimisation 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 organisation's name into Google or another search engine. Your organisation 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 organisation 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.[114] 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.

Clients who find themselves on the end of a complaint should also be prepared to act quickly in order to mitigate any damage done. Also, if the websites in question are accessible in the UK, ISPs and other content hosts could lose any immunity they may have if they are notified about infringing material and take no action.

— CHAPTER 3 —

Copyright (EU)

Chapter Authors

Stephen Edwards, Partner – sedwards@reedsmith.com

Dr. Alexander R. Klett, Partner – aklett@reedsmith.com

Introduction

We have referred to copyright in several of the earlier chapters: in relation to advertising and marketing, commercial litigation, and in the chapter on trademarks, principally with reference to U.S. law and in particular the Digital Millennium Copyright Act ("DMCA"). We thought it would be helpful to pull those threads together and to add specific copyright elements, as well as a European law perspective, so as to provide an overview on the significance of copyright to social media across the continents. Copyright is, after all, at the heart of social media. This chapter will highlight some important differences between U.S. and other countries' copyright laws that companies engaging with social media must have in mind.

In dealing with the position under U.S. law in previous chapters, we make the following points:

- In relation to **branded pages**, we ask rhetorically whether a company can afford not to monitor its branded page for, among other things, copyright infringement, even though the provider of the social media service takes responsibility for responding to takedown notices received pursuant to the DMCA. We explicitly answer that question when discussing user-generated content, where we suggest that companies should have procedures in place if they receive a notice of copyright infringement, not least because (unlike the social media operator) they themselves will not likely have a defence under the DMCA to an infringement claim if they use an infringing work in a commercial context.

- In discussing **defamation risks** and the immunity offered by the Communications Decency Act ("CDA") in the United States, we noted that a blog operator (but effectively any company using social media) cannot assert a CDA defence to claims that are rooted in harm to the victim's intellectual property. In consequence, if the victim asserts, as against the operator, a claim for copyright infringement based on the blogger's uploading of protected material onto the blog, the operator has no CDA defence, and the claim must be resolved under copyright law and in particular the DMCA.

- At the end of the discussion in chapter 12 [10] of the relationship between social media and **trademark protection**, we advise that "it is of the utmost importance to have strategies 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 a claim that they have waived their ability to enforce their ownership rights, while at the same time discouraging others from any unauthorised use of such marks and works of authorship."

If we look at these issues from a European perspective, the same concepts hold good, although it is not the DMCA that governs but rather the E-Commerce Directive[115], as applied by national law in the Member States of the European Union and the European Economic Area. As in the United States, as a general matter, the operator of a social media service is given protection against copyright infringement claims if it operates an effective notice and takedown procedure but, as in the United States, this protection available to the operator may not be available to a company that provides a branded marketing page on which users are able to upload infringing content. Some European courts, such as the German Federal Court of Justice, consistently take the view that while in line with the E-Commerce Directive[116] constant proactive monitoring of sites cannot be expected, an operator has an obligation to prevent subsequent evident infringements by the same infringer.[117] Only in exceptional cases, according to this case law, can an operator be sued to obtain injunctive relief as a precautionary measure if infringements of intellectual property rights on the site of the operator are feared.[118] In general, European courts agree that an obligation to monitor and

review content will only exist for operators of services such as social media services with respect to significant, evident infringements.[119] Companies should therefore have procedures in place to ensure that any evidently infringing material or infringing material they are made aware of by right holders can be removed as swiftly as possible.

Copyright Infringements on Social Media Services

The question of whether the use of third-party content protected by copyright by a user on a social media site constitutes copyright infringement can be answered in a fairly straightforward way. If there is no consent by the right holder, such use will inevitably constitute an illegal act of making the work available to the public under most modern copyright regimes. Most operators of social media services provide in their terms of use that the user is responsible for making sure that material provided by him on the service does not infringe third-party copyrights. As has been discussed above, the interesting question then becomes whether the operator of the service can be held liable and can be asked to stop the infringement quickly, particularly in situations in which the identity of the infringer (the user) is difficult to establish or the infringer is located in a faraway country.

Conversely, however, one can ask whether content legitimately created by users of social media services enjoys copyright protection itself. If this is indeed the case one may wonder to what extent the operator of the service or other third parties may be allowed to refer to, cite or otherwise make use of such content.

Twitter

With respect to tweets, which by definition can be no longer than 140 characters, one may doubt whether they will be sufficiently creative and original to enjoy copyright protection. In many cases, tweets will only consist of short regular phrases that may not be regarded as an original work of authorship in the U.S. sense,[120] an original work in the UK sense[121], or a personal intellectual creation as required under German copyright law.[122] Consequently, in many cases, none of the three regimes will provide copyright protection to tweets.

To the extent Twitter states in its terms of use:

> You retain your rights to any Content you submit, post or display on or through the Services.

this should actually be qualified by indicating that in most cases, tweets will be in the public domain for lack of originality or creativeness. It is not impossible, however, to create short poems or other brief literary works with no more than 140 characters. If originality and creativity can be established, the situation would be different. The analysis would also be different for longer original works broken down into sequences of tweets and made available on Twitter one by one—such as a short story published on Twitter in small bits of no more than 140 characters each, provided the single tweet enjoys protection on its own.

If a tweet or parts of a tweet can be found to be protected by copyright, the use of the respective content by third parties can constitute copyright infringement if fair use (United States), fair dealing (UK), or a similar exception under the respective applicable domestic copyright regime cannot be established. There is no rule, either, under U.S. or European copyright regimes requiring that in order to infringe a literary work, passages of a certain length need to be copied, provided the sequence used enjoys copyright protection as such.

As a consequence, so-called retweeting, (*i.e.*, repeating somebody else's tweet under one's own user name) may constitute copyright infringement as well, provided the earlier tweet is sufficiently original and creative to be protected. Citation exceptions provided[123] may not help in this context as mere repeating of an entire text without incorporating it into one's own original work does not constitute citation.

Facebook, MySpace, et al.

The limitations existing with Twitter with regard to the number of characters do not exist on other social media services such as Facebook and MySpace, among others. The further possibility to upload photographs and/or audiovisual content onto such services leaves no doubt as to the possibility of copyright infringement if third parties copy or otherwise make relevant use without permission of materials taken from somebody's page on Facebook or a similar site.

Terms of Use and Applicable Law for Copyright Law Purposes

Most social media services have terms of use providing for comprehensive non-exclusive copyright licences granted by users to the operator. Typically, such terms of use also provide for U.S. law in the state in which the service is

based. Twitter, for example, provides the following in its terms of use:

> These terms and any action related thereto will be governed by the laws of the State of California without regard to or application of its conflict of law provisions or your state or country of residence. All claims, legal proceedings, or litigation arising in connection with the service will be brought solely in San Francisco County, California, and you consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.

While such terms, if they have been validly made the object of the agreement between the user and the operator of the social media service, may apply for general purposes of international law of contracts, the question needs to be asked whether for purposes of copyright law such a choice of law and venue clause will make all foreign copyright regimes inapplicable.

From a European perspective the answer is clearly: no. According to European case law (and the view of leading European scholars), the posting to social media services of works by users in Europe is governed by the copyright laws of the particular European country in which the user resides, regardless of the contractual regime agreed to in the terms of use. This may be surprising, but it needs to be taken into account, particularly in connection with copyright regimes providing for increased protection for copyright owners, such as under German copyright law.

Moral rights, compulsory remuneration rights, legal limitations on the scope of copyright licences and the prohibition of assignments of copyright provided in the German Copyright Act, for example, will all continue to apply for the benefit of a German right holder or with respect to uses in Germany, even if the operator of the social media service provides for California law. Companies are well advised, therefore, not to be misled into believing that simple choice-of-law clauses, even if they have been validly agreed, will enable them to avoid the much stricter and much more pro-author provisions in certain European copyright regimes, compared with what the U.S. Copyright Act provides.

Music Licensing Issues

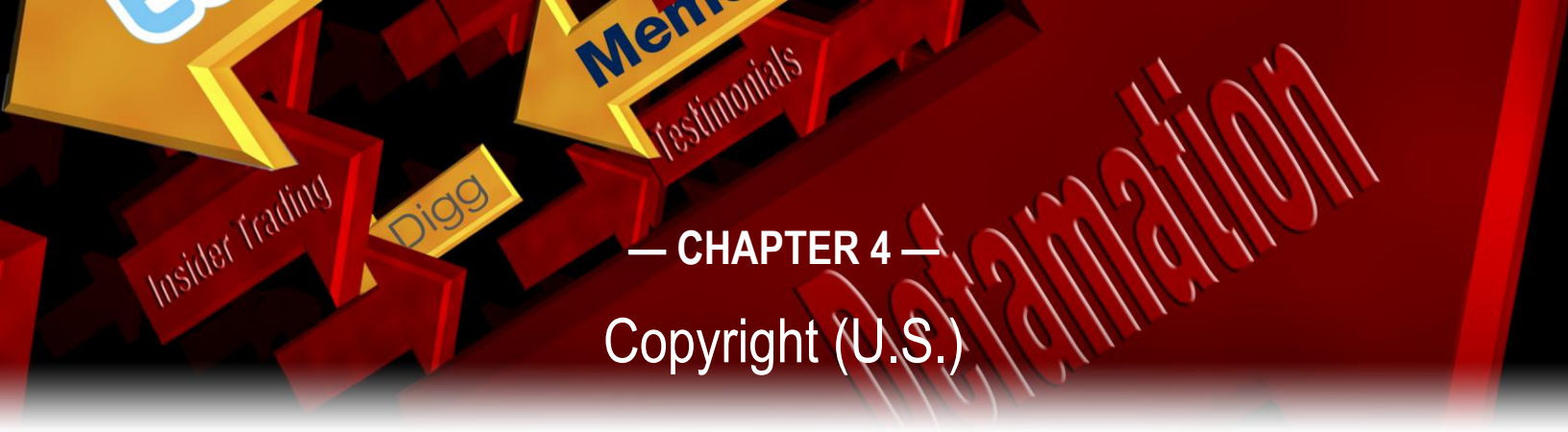
In dealing with the copyright issues faced by U.S. companies engaging with social media in the U.S. market, we did not mention an issue that looms large for European and multi-national companies operating within Europe. If a company wishes to enliven its web-presence by using music, the rights-clearance arrangements that will be needed are very different if the company is operating in Europe rather than in the United States. A U.S. company can usually clear rights for the U.S. market by means of obtaining two or, at most, three licences, from the music rights societies and from the record company concerned. To reach the whole of the EU market, a multiplicity of licences will be needed, in many cases covering only a single country at a time. Only for a very small number of works is it possible to obtain European-wide clearance by means of two or three licences; choose the wrong work and you could be looking at having to obtain 30 or more licences.

Bottom Line—What You Need to Do

- Police your own copyrights and be mindful of copyright protection that may exist for content provided by others. Be aware of the fact that the international nature of global social media services requires that you not only rely on one domestic or one contractually agreed regime, but that you also keep an eye on foreign laws involved with users based abroad.

When clearing rights for using content yourself, be aware of the international scope of the intended use as well, and make sure that you truly obtain sufficient geographic rights for the intended use.

If you operate a site enabling users to upload content, put in place a procedure allowing you to remove, as swiftly as possible, evidently infringing material or material of which you have been told that it is infringing.



— CHAPTER 4 —

Copyright (U.S.)

Chapter Author[124]

United States

Kathyleen A. O'Brien, Partner – kobrien@reedsmith.com

Introduction

This chapter explores the challenges to owners of copyrighted material (commercials, TV shows, films, music, lyrics, stories, articles, books, artwork, web content characters, etc.) created by social media and some strategies for dealing with such challenges.

The rise of social media and the broad reach of the Internet have created a host of new challenges for copyright owners. Digital technologies, including file sharing, MP3s, and digital photos, allow users to link to and display website content out of context while search engines, email, and social media sites enable them to disseminate copyrighted materials in an instant. While greater exposure and better communication with your company's customers through social media can increase brand recognition and reach new markets, it also opens the door to copyright infringement on a whole new level.

The ease with which copyrighted material can be disseminated through social media presents competing considerations for copyright owners: how to adequately protect and preserve the value of your company's creative works without squelching the public dialogue about those works or without alienating your customer base.

The following paragraphs provide an overview of key copyright issues that have arisen, or are likely to arise in connection with, three of the most popular social media sites—YouTube, Facebook and Twitter—and offer some practical pointers for copyright holders on ways to deal with them. We address real-life examples of copyright infringement in social media and how rights owners have responded, and identify key takeaways that rights owners can apply to their own works. We also look at the ways that YouTube, Facebook, and Twitter respond to copyright infringement claims and how they work—or sometimes don't work—with rights owners. Finally, we provide a brief overview of copyright law to help you understand the legal protections that are available to your company.

Social Media in Action in Copyright

YouTube

YouTube, a popular site for sharing video content, has the sixth largest audience on the Internet and attracts 71 million unique users each month.[125] Each day, the viewing public watches more content on YouTube than on TV and cable combined—with more viewers than the Super Bowl.[126] While the size of YouTube's audience and its display of video content present unique marketing opportunities, the unauthorized use of copyrighted material by its users is rampant. Users routinely post copyrighted commercials, music videos, TV shows, and films without authorization. They also use copyrighted material without permission in their own videos in a million creative ways ranging from postings of their kids dancing to a Michael Jackson song, to postings of their cats batting at a Disney cartoon on the TV. YouTube has been the object of media criticism directed at both its routine posting of infringing content and its failure to promptly remove such content.[127]

So what remedies do copyright owners have when the content they own is posted on social media sites? First, it is important to understand the legal obligations that have been imposed on Internet Service Providers ("ISPs") like YouTube, which may help your company to stop infringement. The Digital Millennium Copyright Act

("DMCA") requires ISPs to remove infringing content, upon notice from the copyright owner, in order to avoid liability for copyright infringement. The DMCA also requires ISPs to terminate the rights of those individuals who repeatedly post infringing content online.[128]

Second, it is important to know what tools ISPs like YouTube have made available to copyright owners to help stop infringement. For example, YouTube has created a dedicated Copyright Infringement Notification page where copyright owners can file an infringement notification.[129] In addition, YouTube has created a Copyright Verification Tool that "assists copyright owners in searching for material that they believe to be infringing and providing YouTube with information reasonably sufficient to permit…[it] to locate that material."[130] Finally, YouTube offers a Video and Audio ID program that allows rights owners do the following: (1) identify user-uploaded videos comprised entirely or partially of their content; and (2) choose what they want to happen when those videos are found. Choices including making money from them; getting statistics on them, or blocking them from YouTube altogether.[131]

In an interesting twist, in October 2009, Scribd.com, an Internet-based social publishing company, was sued for copyright infringement by a copyright owner as a result of the very steps taken by the ISP to protect copyright owners from infringement. Elaine Scott, an author, claimed Scribd violated copyright law by retaining an unauthorized "digital fingerprint" of her book in its system and using it to ensure that content from the book was not reposted on its website. When Ms. Scott discovered content from her book on the Scribd website in July 2009, she notified the company of the infringement. As required under the DMCA, Scribd removed that content. However, it also left a "digital fingerprint" of the work in its filing system to help it to identify the book if it was reposted. Scribd did not obtain Ms. Scott's consent to make or maintain this digital fingerprint, or to use her work in this manner.

This lawsuit highlights a Catch-22 for ISPs. On one hand, if an ISP is notified of a violation and does not take steps to remove infringing material, it could be liable for infringement. On the other hand, using a filter system to make a digital fingerprint of the work to identify additional instances of unauthorized use may, itself, constitute infringement. Here, the court must decide whether using part of a work without the author's consent is infringement or fair use. This case is particularly interesting because Scribd is a commercial publishing company and has created a filtering system that could be sold or licensed by Scribed to other similar companies. The case will decide whether an ISP's limited use of a copyright owner's work without the owner's permission, in order to prevent reposting, constitutes fair use.[132]

Finally, your company may wish to consider what steps it can take to encourage consumers to use its copyrighted material in limited ways that are acceptable to it, such as by providing them with specific preapproved content through its company website and/or a social media site. Many companies are starting to create branded YouTube channels that allow consumers to interact with the company in new ways, such as through videos, games, or requests for user video responses to questions.[133] Because the YouTube Terms of Service grant YouTube a license in your company's work, if your company is considering this option, it also should consider negotiating terms with YouTube that permit the company to retain control of its content.

In addition, YouTube Homepage Advertising, a video placement that places your company's video on the top lineup on the YouTube home page,[134] can help your company to direct traffic to its copyrighted pages, and potentially deter consumers from uploading content without your permission. You then can track the traffic to your company's video through the YouTube Insight page, which provides reports and maps of the traffic your company's video receives, broken down by date, time, and global location.[135]

As social media sites like YouTube continue to evolve, it will be important for companies to continue to balance the need to protect their content from infringement against the need to provide consumers with preapproved content to use in their communications about your company and its products on social media sites, so that your company maintains some control and participates in that dialogue.

Facebook

Facebook has more than 350 million active users.[136] If Facebook were a country, its user base would make it the fourth largest country in the world. The enormous marketing opportunities presented by Facebook cannot be denied. These opportunities are not just domestic – about 70 percent of Facebook users are outside of the United States.[137] Further, there are more than 65 million active users currently accessing Facebook through their mobile devices, and the people who use Facebook on their mobile devices are almost 50 percent more active on Facebook than non-mobile users.[138] Not only can copyright infringement occur and proliferate quickly, but it can also be difficult to identify infringers. As a rights owner, this is not all bad news. Facebook is a great forum in which your

company can monetize or share its work. However, you should understand how your company can stop infringement and think creatively about how to guide the use of its work in this medium before users take control.

Facebook offers various levels of copyright protection and remedies for infringement.[139] For example, the site provides both an automated DMCA form that your company can use to report copyright infringement,[140] and it has a procedure in place to appeal such claims.[141] Though Facebook's enforcement of these policies is sometimes criticized, for the most part, these are viable and effective remedies.[142]

The key to copyright protection on Facebook is to monitor the dialogue, to think creatively and to respond quickly. A company that fails to take immediate action may lose out on unique marketing opportunities that may only exist for a fleeting amount of time. Take, for example, Hasbro's response to *Scrabulous*, a thinly veiled online version of Hasbro's *Scrabble* that was a major Facebook favorite in 2006-08.[143] Not surprisingly, the game and related application became the focus of an infringement lawsuit, which ultimately resulted in the removal of *Scrabulous* from Facebook; a lot of angry fans; the (not-as-successful) launch of Hasbro's *Scrabble* application; and a re-branding and re-launch of what was formerly known as *Scrabulous*. One of the main reasons *Scrabulous* became so popular is because there was no "real" *Scrabble* on the site. Unfortunately, Hasbro missed out on a major opportunity to interact with and engage their audience in social media here by promptly providing a *Scrabble* application to fill that gap. Hasbro waited until two years after the developer of *Scrabulous* began exploiting Hasbro's copyrighted game, made a profit, and gained the support of a broad swath of the Facebook audience, to respond with its own version. By the time the Hasbro finally launched its application, there had been too much controversy around *Scrabble*, and fans had moved on to other games. A month after the *Scrabble* application hit Facebook, there were only 8,900 active users, compared with the half-million-a-day users of *Scrabulous* the day Hasbro filed its lawsuit.[144] Neither *Scrabble* nor *Lexolus*, the new non-infringing version of *Scrabulous*, have recovered. In January 2010, *Farmville* was the most popular game on Facebook, and *Scrabble* does not even crack the top 15.[145]

Rights owners should also note how Facebook itself handled the controversy. While Facebook claimed to be a neutral platform provider, many commentators questioned this neutrality.[146] It was in Facebook's interest to keep the game available on its site because it had a cross-generational appeal, and people could browse other Facebook pages while waiting for their opponent's move. Any public relations fallout from pulling the game would have negatively impacted the site. Because the legal standards related to games are not as strict as those related to digital music or movies, Facebook was able to walk the line legally and err on the side of its platform developers.

The *Scrabulous* debacle should serve as a lesson to copyright owners: pay attention to what social media users are doing, act quickly and be creative. Doing so will not only protect your copyright, it can enhance the positive buzz about your company and its products, and can help your bottom line.

Twitter

Twitter is currently the fastest-growing social networking site out there. Twitter grew 1,382 percent year-over-year in February 2009, registering a total of just more than 7 million unique visitors in the United States for the month.[147] As noted in the Trademarks chapter, Twitter provides unique, immediate marketing opportunities,[148] but real risk of infringement of your company's intellectual property as well. Unlike a traditional social media site like MySpace or Facebook, Twitter is a microblogging site that allows users to send and view short messages called *tweets*. Tweets are text-based messages limited to 140 characters in length that are posted on a user's page and viewable to the entire world. Users can also restrict their tweets so they are viewable only to their friends, who are called *followers*. Users can tweet via the Twitter website, SMS, or smartphone applications.

For now, Twitter's Terms of Service tend to follow the mold of other social media sites, with standard DMCA takedown requirements and disclosures. Twitter's Terms of Service note that a user maintains ownership of her content, she grants a license to Twitter "authorizing [Twitter] to make [her] Tweets available to the rest of the world and to let others do the same."[149] Twitter's stated Copyright Policy is as follows:

Twitter respects the intellectual property rights of others and expects users of the Services to do the same. We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. … We reserve the right to remove Content alleged to be infringing without prior notice and at our sole discretion. In appropriate circumstances, Twitter will also terminate a user's account if the user is determined to be a repeat infringer.[150]

For copyright holders, such as authors, journalists, newspapers, screenwriters, lyricists, photographers, artists, and other holders of copyright in written and visual works, Twitter presents some new and novel challenges. By the nature of a Tweet, a user is more likely to get in trouble for defamation or libel than for copyright infringement.[151] However, as journalists and individuals begin to use Twitter to report during a political protest, such as those following the Iranian presidential election in June 2009 when the government shut down phone and Internet service,[152] or during a national disaster, like the earthquake in Haiti, copyright issues arise.

The unauthorized use of photographs posted via Twitter is the first opportunity the courts will have to examine copyright infringement on the site. In April 2010, Agence France Presse (AFP) sued a photojournalist in the U.S. District Court in New York, for "antagonistic assertion of rights."[153] The photojournalist took an iconic photo of a woman staring out from the rubble in the aftermath of the Haiti earthquake, which he posted on Twitter via TwitPic, a Twitter-compatible—but separate from Twitter—photo sharing application. The next day, his image was picked up by AFP and Getty Images, and appeared on the cover of several publications and websites. The photojournalist never authorized AFP to use or distribute his images, and sent strongly worded cease-and-desist letters demanding payment. AFP claims that because he posted the images on Twitter, he is bound by Twitter's terms of service, and that he had granted a nonexclusive license to use, copy and distribute his photographs. The AFP's case relies on Twitter's Terms of Service, which primarily address text-based tweets, not content linked to the site via another application. TwitPic has its own Terms of Service. The outcome of this case may change the way journalists and photographers share breaking news and information on social media. It will also inform how the courts approach copyright infringement on Twitter.

This case still leaves open two major questions with regard to Tweets and copyright law: (1) are pure text-based Tweets themselves copyrightable expression, and (2) can text-based Tweets infringe copyright ownership? At the moment, there is certainly potential for copyright infringement, but there are more questions than answers. A user may quote portions of your copyrighted work without attribution, which may be subject to the fair-use defence for an individual Tweet; but what happens if a user starts posting your entire novel, 140 characters at a time? Will a court look at the individual Tweets, or will it look at the larger conversation and context? Is one Tweet part of a longer document, or is each Tweet a separate event? What happens when users use your graphic design as their background on their Twitter pages, or as their personal image in their profile? If a Tweet is in fact copyrightable, is re-Tweeting, reading a Tweet, displaying full Tweets on other sites, or quoting a Tweet in a news story, fair use? Each of these actions copies the entire expression in the original Tweet. The Tweet was posted on a public site by a user who knows it "may be viewed around the world instantly," and the user agreed via the Terms of Service that her tweets could be re-Tweeted, etc. Although these questions fall clearly within the realm of copyright infringement, the courts and regulators have not addressed them.

Users are beginning to question the copyrightablility of their Tweets. For example, in spring 2009, Mark Cuban, owner of the Dallas Mavericks, was slapped with a $25,000 fine by the National Basketball Association ("NBA") for tweeting during a game about a bad referee. When ESPN republished his Twitter feed without his permission, Cuban got mad and raised questions about the propriety of ESPN's act on his personal blog.[154] Under Twitter's Terms of Service, however, by posting your Tweet, you allow Twitter to broadcast your comment to the entire world, and allow anyone to re-Tweet your comment. ESPN was fully within its rights to repost, but this kind of commentary among the Twitterverse will undoubtedly stir up legal issues.

Like the rest of the Twitter/copyright relationship, it is unclear whether a Tweet that is not quoting from a protected work is copyrightable expression. There is a plausible argument that a Tweet could be copyrighted if it is an original expression, it is not in the public domain, and is not licensed, either explicitly or implicitly. In order to be copyrightable, a Tweet must be sufficiently original—not just a statement of fact or the sharing of information.[155] Generally, there are two aspects to originality: independent creation and a modest quantum of creativity.[156] As a general proposition, mere words and short phrases, even if they occur in an original copyrighted work, do not themselves enjoy copyright protection.[157] Moreover, titles may not claim copyright protection.[158] At only 140 characters, a Tweet is likely too short and too superficial to be an original expression. If a Tweet is a slogan, there is some argument that the short phrase could be trademarked. (*See Chapter 14 – Trademarks.*)

At least for now, copyright owners should not expect full and complete rights in what they post on Twitter. These are all issues that have yet to be decided directly by a court, and it is as yet unclear how well developed Twitter's plan for dealing with copyright infringement is, or how well enforced. As a result, a copyright owner must be active

about protecting her rights, and must think about how (or whether) Tweets can damage your copyright interests. Determine a standard as to your opinion of objectionable use of your material, and use the copyright infringement policy to your advantage. As the Twitter Terms of Service say, "What you say on Twitter may be viewed all around the world instantly. You are what you Tweet!"[159]

Current Legal and Regulatory Framework in Copyright

Creative Commons Licenses

Creative Commons is a nonprofit organization dedicated to expanding the range of creative works available for others to build upon legally and to share.[160] They provide licenses to mark creative work and to allow an author to decide how others can use, share, remix, or use their work commercially.[161] These licenses give creators and content owners a way to grant copyright permissions to use their works. In the interest of sharing, collaboration, and access to creative content, Creative Commons licenses essentially enable content owners to change their copyright terms from "all rights reserved" to "some rights reserved."[162] The rights reserved are up to the content owner.

Creative Commons licenses are becoming a popular alternative to traditional copyright licenses, particularly on the Internet.[163] Many individual photographers, writers, and musicians who are not associated with an agency or a label now are using Creative Commons licenses to share and protect their works. These licenses allow creators to grant broader access to their works. Musicians, bloggers, and artists are signing on to the idea of greater public access to information through licensing. New industries continue to accept Creative Commons licenses, so the impact of this shift may be significant. A blogger, for example, can select from seven different licenses, choosing which protections of traditional copyright licenses he wishes to apply to his work, and which he is willing to waive.

In the publishing and music worlds, Creative Commons licenses are becoming more and more common. In August 2009, Google Books launched a program to enable authors to make their Creative Commons-licensed content available for the public to share, download, remix, and use. In May 2009, the band Nine Inch Nails released a "one hundred percent free" album to fans under a Creative Commons license. The band told fans

> 'we encourage you to
> remix it
> share it with your friends,
> post it on your blog,
> play it on your podcast,
> give it to strangers,
> etc.'[164]

All tracks are readily remixable via their audio source files that are available on the page.[165] Also, in contrast to services that prevent the re-distribution of tracks, all of these files are 100 percent DRM-free. This alternative path for artists to distribute their music creates a substantial challenge to the music industry, and essentially forecloses any copyright claims the band may have regarding the use of this content in the future.

The problem with these licenses is that content creators do not necessarily understand what rights they are getting or giving up. For example, a photographer uploaded pictures of his trip to Australia to his Flickr account. He later found them used in an Australian travel ad campaign. Though he was upset that the photos were used without his permission and without any payment, he lost his case because he used a Creative Commons license that granted use rights to the public. Thus, companies who chose to grant a Creative Commons license must be sure that they understand exactly what use rights they are granting to the public since they will no longer be able to reap the monetary benefits of the exclusive right to use that content in the future.

The Law Behind Copyright

In general, content on the Internet is protected by the very same copyright laws that protect content off-line. So far, the courts have not expanded the fair use defense to allow for the unauthorized use of copyrighted content by users on social media sites. The Internet does make it more difficult for companies who own copyrighted material to control the unauthorized distribution and use of such works, and may make it harder to identify the infringer and hold him accountable.

What is a copyright? According to the U.S. Patent and Trademark Office,

A Copyright is a form of protection provided to the authors of "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished…. The owner of copyright [has] the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the

copyrighted work publicly, or to display the copyrighted work publicly. [166]

A copyright protects the manner in which you express an idea, or the "form of expression rather than the subject matter of the writing."[167] It does not protect the underlying idea or information. For example, your company's original description or photograph of a clock could be copyrighted, but your copyright only prevents others from copying your specific description or photograph; it does not prevent them from writing their own description, taking their own photograph, or using the clock. The copyright on Kermit the Frog, for example, restricts others from making copies of or derivative works based on the Kermit character, but it does not prevent others from anthropomorphizing a frog. Likewise, there is no copyright protection for the idea of a hidden camera consumer taste test, but what can be protected is the actual dialogue, copy, layout, photography, music, or other actual expression used by your company in that format.[168]

Copyright law prohibits third parties from creating derivative works based upon a pre-existing work without the copyright owner's permission. To establish copyright infringement in any context, the owner of the copyright must prove that he owns a valid copyright in the material and that the defendant has reproduced, distributed, or publicly displayed protected elements of the work, or has created a derivative work based on the copyrighted work without permission.[169] In the context of computers, mobile devices, and the Internet, the unauthorized transfer of a computer file representing the copyrighted work, or from which the copyrighted work can be reproduced with the aid of a machine, is copyright infringement.[170]

Copying is established when the copyright owner shows that the defendant had access to the copyrighted work and there is a substantial similarity between the copyrighted work and the defendant's work.[171] Because the standards by which copyright infringement are judged are so subjective, each case must be decided based on its individual facts. Courts tend to analyze an advertisement to determine whether the allegedly infringing ad captured the "total look and feel" of the allegedly infringed work. This means that the court will look not only at the individual elements of the pre-existing work, but also at the aggregate appearance of the work to determine whether there is "substantial similarity" between them.

Because copyright infringement cases are so fact-specific, there is no bright line rule as to the amount of copying that constitutes copyright infringement. Some cases have found copyright infringement even where only a small portion of the text has been copied. For example, a court found copyright infringement where only 3-6 percent of the overall material had been copied.[172] In that case, the defendant published a book of trivia questions and answers about the "Seinfeld" television show. Only a small portion of each episode, including quotes and situations, was included in the book. Although the court did not find that the defendant had violated the "Seinfeld" copyrights based on the quantitative component, the court focused on the qualitative component, finding that each question was "based directly upon original, protectable expressions in Seinfeld."[173]

In another case, the same court held that a defendant had not infringed works where it copied approximately 20 percent of the overall material.[174] In that case, the defendant copied approximately 22 abstracts from the plaintiff. Although the court found copyright infringement in 20 of the abstracts, the court concluded that two of the abstracts did not infringe Nikkei's copyrights, but for two very different reasons.

In the article that copied the 20 percent of the plaintiff's original work, the court found that the quantity of the copying did not constitute infringement given the "nature" of the articles, namely that they consisted "almost entirely of [plaintiff's] reporting of unprotected facts . . ."[175] In the other abstract, the court found no infringement of plaintiff's original work, as the defendant did not copy the abstract itself. The court determined that "by incorporating [plaintiff's] abstracted facts into *new and original sentences*, [the defendant] stay[ed] well clear of qualitative infringement even though the abstract use[d] nearly all of the facts contained in the corresponding article."[176]

Fair Use

The fair use doctrine is an affirmative defense to copyright infringement that limits the exclusive right of the copyright owner to reproduce the copyrighted work.[177] While the fair use defense is also fact specific, the Copyright Act provides the following illustrative list of factors to be considered in determining whether a defendant's use of the work constitutes a fair use: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[178]

Bottom Line—What You Need to Do

Although social media presents a new and ever-expanding forum in which to disseminate copyrighted material, copyright owners can use a variety of tools to protect their copyrighted works without squelching consumer interest. It is possible to walk the line between protecting your copyrighted works, encouraging public dialogue about your works, and maintaining a good relationship with your customer base. We encourage copyright owners to understand and participate in social media. Pay attention to how users seek to use and interact with both your copyrighted material and similar types of material offered by others. Be creative and consider new ways your work can be used in social media. If you discover your rights are being infringed in material ways that jeopardize your company's rights or rob it of its profits, respond quickly in a way that is sensitive to the medium.

— CHAPTER 5 —

Data Privacy & Security

Chapter Authors

United States

Mark S. Melodia, Partner –mmelodia@reedsmith.com

Paul Bond, Partner – pbond@reedsmith.com

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

United Kingdom

Cynthia O'Donoghue, Partner – codonoghue@reedsmith.com

Gregor J. Pryor, Partner – gpryor@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,[179] there are more than 400 million active users of Facebook worldwide. Most major brands have Facebook group and/or fan pages—with commentators even doing case studies of those that have been most effective.[180] Yet, there remains 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.[181] 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 using their mobile phones, and stories accompanying pictures of overflowing toilets instantaneously appeared in social media. Similarly, when a group of unfortunate passengers were stuck in the Channel Tunnel for several hours during adverse winter weather, Facebook updates told the story of their difficulties. Just as these incidents spread virally via social media, so too might the liability associated with a breach of protected personal information. In the United States, millions of dollars in claims could be made against the hosting site and cause extremely bad publicity. The prospects for further government regulation of social media in the United States. are accelerating. Prompted by the expansive new information sharing practices of social media companies, both the Federal Trade Commission ("FTC") and the United States Department of Commerce are looking into the development of formal standards to protect the privacy of Internet users.[182] The adequacy of the traditional framework of providing notice to consumers about privacy practices and relying on the consumer's informed choice is coming under increasing skepticism.

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.[183] Even standard business processes pose risks to personal data. Not forgetting that social media companies themselves want to gain commercial leverage from the data collected.

Social media enterprises collect, store, use, share, and dispose of personal data every day, including eCommerce-related non-public financial information (for example, 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. This chapter explains 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 recognise the increased importance privacy and data protection play—not only in law and regulation, but also to consumers. In Europe, regulatory guidance suggests separating terms of use and terms relating to data protection and privacy. 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 transparency and consent 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.[184] 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 site or service. So, access to and data from users in the community is a social media company's primary commodity to monetise the site.

This ability to commercially exploit data is tempered by data protection and privacy laws. The need for 'information monetisation' can create in an adversarial relationship between the site user and the social media company. As a result, many consumer advocacy organisations are analysing and notifying consumers of updates to social media website user agreements.[185] These consumer watchdog organisations can generate considerable controversy; take for example, Facebook's Terms of Service update in February 2009. At that time, *The Consumerist* flagged a series of changes to the Facebook Terms of Service, including deletion of the following text:[186]

> 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.

The Terms of Service change is not the only example of the tension created over the use of consumer information and consumer disclosures. In the early days of 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 were 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.[187] In less than ten days, this group gained 50,000 members. Beacon amended its Terms of Service as a result.[188] A class action lawsuit was filed against Facebook as a result of Beacon. The lawsuit was ultimately settled in September 2009[189], and the Beacon advertisement service was shut down.

Facebook has, nonetheless, continued to press on the outside of the envelope with respect to consumer privacy. At the F8 Conference this April, Facebook announced a series of changes to its privacy policies sure to draw considerable attention.[190] The changes include:

> Allowing external websites to add a "Like" button. If the user of that external website clicks the "Like" button, that user's Facebook page will be modified to reflect information about the user's use of that external site. The user's Facebook friends will be able to view such information.
>
> Partnering with sites like Pandora and Yelp! to provide for "instant personalization." This means that when a Facebook user visits those sites, unless she has taken specific elections on her Facebook privacy settings, those sites will download "can pull in information from your Facebook account, which includes your name, profile picture, gender and connections (and any other information that you've made visible to the public). If you visit Pandora, for example, the site could also pull in your favorite music artists, create playlists accordingly, and then notify your Facebook friends."[191]

In the immediate aftermath of the Facebook changes, members of the United States Congress have already expressed intent to pass laws putting the onus on companies like Facebook to get specific consent from consumers before rolling out new information sharing platforms.[192]

Compared to the United States, Europe has traditionally taken a more stringent approach to data protection. Article 8 of the Charter of Fundamental Rights of the European Union explicitly provides a fundamental right to protection of personal data within the EU. There is also a greater focus on raising awareness. For example, Europe even organised a "European data protection day", held annually on 28 January.[193] As a result, social networking sites tend to be the subject of far greater public scrutiny than in the United States. Privacy groups and thorough press coverage ensure that any changes to the privacy policies of service providers and any risks or abuses related to these services are comprehensively discussed and brought to the attention of social media users. The Guardian story covering the changes to Facebook's Privacy Policy in 2009 titled "Facebook privacy change angers campaigners"[194] and a headline from The Sun titled "Teen Weapons Shock On Bebo",[195] are just two examples of the press coverage social networking sites receive.

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 information that may be detrimental to Starbucks or any brand 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"[196] it sends to its followers, but the company cannot directly control what is "retweeted"[197] by others from the company-sponsored tweets.[198]

For portals or fan sites that are not sponsored, 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 site's user agreement. These will be different depending on the site or service. 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.[199]

Alternatively, companies could issue cease-and-desist e-mails directly to the employee posting the content on YouTube.

- **On Facebook the answer is possibly.** On Facebook, the remedy for removing content is reporting abuse of Facebook's Statement of Rights and Responsibilities (the "Terms").[200] In Section 5 of the Terms, Facebook will not permit posting of "anyone's identification documents or sensitive financial information on Facebook."[201] Depending on the content of the private information disclosed in the videotaped 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.[202] 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.[203] 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 removal of some content by social network providers from the service, it may still surprise some users how their data is stored and used by social networking sites, even in some cases after it has been removed or the user is no longer a member of the site. In addition, social media sites employ technological measures that recognise a user's computer. For example, according to Twitter's terms of use, Twitter can collect and use a user's "automatic" information, such as a user's IP address or cookies. Whether these provisions will be sufficient to satisfy the upcoming changes in law which will require Twitter to obtain European users' consent before using their cookies remains to be seen.[204]

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

US position

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 epitomises that modern, global ethos.

Every jurisdiction in the world can claim the right to protect its citizens–and information about them. The United States has a very different concept of "personal information" and adequate protection of it than the European Union; the European laws are not necessarily across all of its Member States. 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. By way of example, 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."[205]

Europe position

Social media services accessible in Europe will also have to comply with the relevant legislation, the implementation of which may differ between Member States. They may also be subject to any additional national measures.

The EU's Article 29 Data Protection Working Party has set forth an opinion on online social networking.[206] 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. However, 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."[207] The Working Paper goes on to state a number of other positions regarding marketing by SNS, complaint procedures, and (advocating) the availability of pseudonyms.

United Kingdom position

The UK has its own domestic data protection law in place which implements the EU Data Protection Directive.[208] The Data Protection Act 1998 ('Act') requires organisations processing personal data to comply with eight distinct data protection principles. The UK also has in place domestic legislation implementing the EU e-Privacy Directive.[209]

The UK Government is currently at odds with the European Commission for failing to properly implement the Data Protection Directive and e-Privacy Directive at national level. The European Commission commenced infringement proceedings against the UK for its failure to guarantee the confidentiality of electronic communications (such as emails and internet browsing) which protection is otherwise enshrined in European legislation. This action was triggered by secret trials conducted in 2006-2007 by the UK telecommunications provider, British Telecom, of a behavioural advertising technology being developed by the company Phorm. This technology enabled the monitoring of an individual's Internet use without the user's consent or knowledge, the results of which enabled companies to more effectively target advertising to users. In a failed attempt to bypass data protection laws, Phorm matched a user's IP address with a unique identifier which was then provided to advertisers, together with profiling information about browsing history. If the UK fails to change its domestic legislation to ensure the privacy of online communications, this action may result in a hearing before the European Court of Justice.[210]

Privacy Policies/Notices: Guidance and General Principles

On both sides of the Atlantic surveys have been carried out to assess whether privacy policies sufficiently and clearly inform users of how their personal data will be used and for what purposes. Although in the UK privacy policies are not a legal requirement under the Act, a privacy policy is a simple way to satisfy the fair processing requirement, which is one of the data protection principles under the Act. Regulatory guidance supports the use of clear and simple privacy policies which adapt a "layered" approach, with the most important information highlighted in a clear manner.

Nonetheless, the surveys have highlighted a need for existing privacy notices to be clearer and more user-friendly. As a means to an end, organisations should make sure that their privacy policies focus primarily on informing the consumer and not on protecting the entity.[211]

Privacy policies should be reviewed regularly to make sure that they continue to comply with any changes in the data processing activities of an organisation and the relevant data protection and privacy laws applicable.

There are obvious benefits to ensuring privacy policies are transparent. Not only will consumers be less likely to complain, it may also provide a competitive advantage from consumers having more confidence in the organisation and how their personal data is being processed. This may lead to consumers entrusting the organisation with further personal data it would not otherwise have received. This seems to be one of the most important trends in social media today – do users trust the site operator?

The Next Direction in Privacy Law [212]

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 US 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 shut down its Beacon program and donated $9.5 million to a non-profit foundation to promote online safety and security.[213] 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 capitalising 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 realise 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 global 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".[214] 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

FTC that unless the industry adopted polices, government regulators would step in.

The industry effort covers the categories the FTC 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.

This initiative appears to have now crossed over to Europe and there is discussion of a special "behavioural" advertising logo that will be displayed in all behavioural advertising. Looking forward, privacy and data protection law will continually be outpaced by technological developments. To take a recent example, the Google Buzz social networking service that was launched in February 2010 has been at the centre of a torrent of criticism by users and privacy groups who claim that the new service has violated rights to privacy. Google Buzz was an attempt by the search giant to convert its Gmail service into a social network. A particularly controversial feature was that Gmail users were automatically signed up to Buzz and a 'ready-made' social network of 'friends' for them to follow was created using information from Gmail accounts of the contacts with whom they most frequently email and chat.

Following the ferocity of public reaction, Google has been forced to adapt many of the features of Buzz, including removing the automatic links between Buzz and content posted by users on other Google services (*e.g.*, Picasa photo albums), making the option to opt-out of Buzz altogether more prominent in the email facility and adopting an 'auto suggest' rather than an 'auto-follow model'. In April 2010, the Privacy Commissioner of Canada, Jennifer Stoddart, and the heads of the data protection authorities in France, Germany, Israel, Italy, Ireland, Netherlands, New Zealand, Spain and the United Kingdom sent a strongly-worded letter to the chief executive officer of Google Inc. to express their concerns about privacy issues related to Google Buzz.[215]. The authorities noted that:

"While your company addressed the most privacy-intrusive aspects of Google Buzz in the wake of this public protest and most recently (April 5, 2010) you asked all users to reconfirm their privacy settings, we remain extremely concerned about how a product with such significant privacy issues was launched in the first place." And, in a statement seemingly directed at every company looking to launch innovative products in this space, the regulators warned, "It is unacceptable to roll out a product that unilaterally renders personal information public, with the intention of repairing problems later as they arise. Privacy cannot be sidelined in the rush to introduce new technologies to online audiences around the world."

Whilst legal action by users who feel their rights have been infringed is inevitable (for example, a woman in Florida has already instructed lawyers regarding the misuse of her personal data), the problem for Google may spread far wider. In trying to make the "getting started experience as quick and easy as possible"[216] to compete with other social networking services, they have potentially alienated users and may now have a harder task convincing the millions of users on Facebook and Twitter to migrate to Buzz instead.

Another social media phenomenon is the exploitation of geo-location technology. Four Square is a location-based game which can be downloaded onto a user's phone and which turns city maps into a game board. Users can "check-in" via their phones and this information is fed to Twitter, where the user's location is made public. By "checking in," the application is able to recommend places to go, things to do nearby and tips from other users for that location. Whilst this application clearly has its benefits, users appear undeterred by the implications of revealing their whereabouts, or, indeed, where they are not; this could pave the way for a new wave of privacy concerns.

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.[217]
- 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.[218]
- A Canadian court allowed discovery of a Facebook profile in a motor vehicle accident suit, despite the document being subscriber-designated as limited access.[219]
- 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.[220]

- Subscribers' posts may violate their own company's privacy policies, or even reveal their own company's trade secrets.[221]

- Subscribers may later regret their social media postings, but the evidence that those posts were made can be crucial and published if there is a public interest justification.[222] 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.[223]

- 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.[224] The UK Courts are following New Zealand and Australia having recently allowed an injunction to be served on a defendant through Twitter for the first time.[225]

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.

Ultimately, subscribers should also take steps to protect themselves because regulators can do only so much to protect subscribers' personal data and privacy.

Children

The popularity of social networking with young people makes the issue of data protection and privacy more acute. A central concern is that young people lack the awareness of the associated risks of these services and the potential for abuse when revealing personal data. Online risks for young users include illegal and age-inappropriate content, improper contact and conduct, including victimisation or grooming and potentially risky behaviors. Whilst the United States has laws and regulations to protect the privacy of children online, the FTC has announced plans to accelerate review of its regulations with an eye towards imposing more stringent standards.[226]

The impact of digital media on privacy issues for young people has been a key focus in both the UK and throughout Europe. In the UK, for example, the Information Commissioner has published numerous good practice notes for website operators whose sites are directed at children. The Home Office Task Force on Child Protection on the Internet has also published in 2008 good practice guidance for providers of social networking and other interactive services[227].

Whilst a focus of legislators has been to raise awareness amongst users of the risks associated with social networking (for example, through the annual EU "Safer Internet Day"), more recently there has been a focus on the contribution that service providers can make to security in the online environment. Following almost a year of discussions, in February 2009 the European Commission and major social networking companies, including Facebook, Bebo, and MySpace, agreed the "*Safer Social Networking Principles for the EU*"[228]. These principles were aimed at giving young people extra protection from violations of their privacy and the potential abuse of their personal information. Key principles include: ensuring services are age-appropriate for the intended audience[229]; empowering users through tools and technology to manage the service[230]; providing easy-to-use mechanisms for users to report conduct or content that violates the Terms of Service of the provider; encouraging users to employ a safe approach to personal information and privacy; and assessing the means for reviewing illegal or prohibited content.

However, a year on, the review of the implementation of the principles published by the European Commission on 9 February 2010 suggests that whilst the principles have been a step forward in tackling online risks for young people, more still needs to be done. According to the Commission less than half of social networking companies make profiles of users aged under 18 visible only to friends by default, and only one-third replied to user reports requesting assistance.[231] Whilst currently the Commission is in favor of a multi-stakeholder collaboration with providers and adopting a 'best practice approach' to manage potential risks, if providers do not toe the line, the consequence may be regulatory intervention.

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.

The penalties for breaches of the Data Protection Act 1998 in the UK are currently under review.[232] The UK Government has proposed to put in place tougher sanctions to act as deterrents, for example, up to two years imprisonment and maximum fines of £500,000, the latter of which is expected to take effect in April 2010.[233] The UK, as well as other European countries, is taking data protection law seriously, and service providers should bear this in mind.

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[234] and have been sexually assaulted,[235] among other crimes. Attempts have been made to hold the social media enterprises themselves liable for not doing more to stop these abuses. Whilst 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.[236] 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.[237]

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 6 – 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."[238] 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."[239] 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.

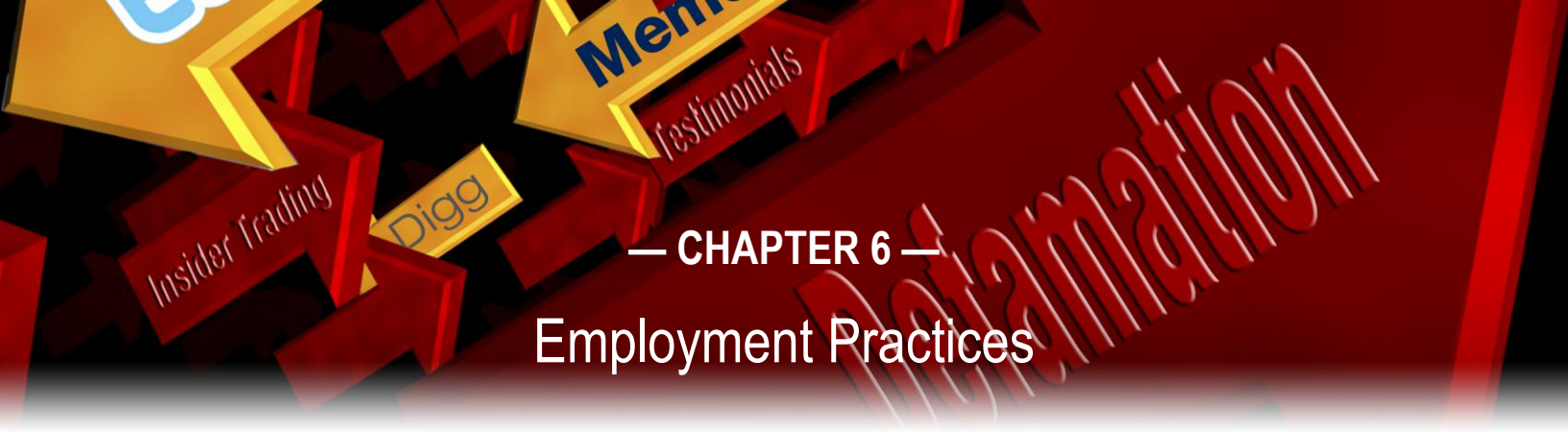
Also, like every company, social media companies should have plans for: the protection and secure disposal of personal data (including in hard copy); the implementation of major litigation holds; and response to the loss or theft of personal data (including, where required or appropriate, through notice 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. Recognise 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 6 —

Employment Practices

Chapter Authors[240]

United States

Eugene K. Connors, Partner – econnors@reedsmith.com

Sara A. Begley, Partner – sbegley@reedsmith.com

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

United Kingdom

Laurence G. Rees, Partner – lrees@reedsmith.com

Carl De Cicco, Associate – cdecicco@reedsmith.com

France

Nicolas C. Sauvage, Partner – nsauvage@reedsmith.com

Introduction

With apologies to Will Shakespeare, quite the networker himself in Elizabethan times, to net or not to net is NOT the question. Because networking is virtually pandemic these days, the real question is not whether, but where, when and in what ways, should we net with each other to achieve networking benefits and avoid its misuses. Because most networkers are employees, the follow-up question, addressed here, is how far can and should employers go to "guide" and "monitor" employee networking "choices," and work to prevent and reduce the broad and ever-growing scope of problems and liability arising from the use of social media in the employment context.

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.[241] 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.[242] 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.[243]

While there is currently no specific statute codifying the law regarding use of social media in the employment arena, employers should look to their current electronic use policies, as well as to the laws and guidance developed over the past several years regarding best practices for company and employee use of electronic media involving email, Internet, BlackBerry, other PDA and cell phones, and confirm that the policies in place are sufficiently broad to prevent, or at least limit, abusive use of social media by the employees. Relevant policies naturally draw from the established principles of maintaining proper workplace environment and establishing reasonable restrictions on employee behaviour. Examples include: employee privacy, both on and off site, as well as consent issues relating to workplace searches; adherence to anti-discrimination and harassment law protection of company trade secrets and other intellectual property tenets; and prevention of defamation, tortious interference with contractual relations or unfair trade practices. The most prudent course to protect against liability in the employment realm is to examine

each policy that guides the behaviour and conduct of employees, and modify, where required, to create an organic document that broadly interprets this burgeoning form of communication and publication.

Social media may be utilized by companies in a variety of imaginative ways related to employment. As we know, social media is a powerful recruitment tool that can be used to create a buzz or intrigue about the employer and connect heavily recruited talent with the company. It is now de riguer for employers and recruiters to "online" a prospective candidate by scanning his or her LinkedIn, Plaxo, Facebook, Twitter, or other business or social networking pages. It can also be used to educate employees and the public about company advances, enhance PR, respond to negative press, and detect theft or misappropriation of trade secrets, abuse of overtime, sick leave or fraudulent medical claims by employees. As discussed below, these online resources can provide valuable information and an immediate global connection with the public, but must be used consciously and appropriately by both employers and employees to avoid legal misuse.

Misuse of social media can be devastating to a company, both legally and from a public relations perspective. Social media employee banter relating to protected traits such as race or gender may violate an employer's anti-harassment policy and create a hostile work environment, just as it does when communicated in person by employees. An employee's tweets about the employer's new R&D project may result in leaking valuable proprietary and trade secret information. An online smear campaign about a competitor's product by an employee can subject an employer to an unfair trade practices or tortious interference claim. A manager's online gossip about an employee's purported drinking problem that proves to be false may result in a defamation claim. Employees griping via social media about their work environment can not only impact the employer's reputation, but also potentially provide a window for the employer into employee morale and its potential negative impact on productivity. Finally, an employer's "inattention" to online behaviour by employees can make it legally liable, if it knew, or should have known, of the behaviour, but failed to take adequate measures to correct the situation, or to notify the appropriate authorities. These concepts should all be familiar to employers. The social media phenomenon merely adds a new, albeit infinitely expansive, arena in which employment issues can arise. Put simply, online "talk" by employees has created a hornet's nest of new challenges for employers. The legal principles and best business practices employers should use to face these challenges remain the same as those they have used to monitor and control other technology advances that increase the speed and amount of communication among employees, such as email, texting or any other such medium.

This chapter provides companies with an overview of how social media affects the workplace and the resulting issues to consider and manage in connection with employee use of social media. We begin by examining the possible uses of social media by employers and then turn to use by employees, and end with 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 companies create and use social media sites for everything from marketing promotions (*See Chapter 1 – Advertising & Marketing)* to attracting job applicants. Such uses are arguably the most acceptable and productive for a company. To minimize legal risk, companies should reasonably and consistently monitor sites for derogatory or otherwise harmful content, and, when it occurs, remove it immediately, block the offending author, and take curative action. Because the company controls the site, such action should be simple and quick.

Does or should your CEO have a Facebook or other social media presence? Sometimes a CEO may create his/her own social media page to market the company or "counter" harmful media blasts. At other times, it may be strictly personal with nothing to do with the company. It is sometimes difficult to discern whether a CEO's social media page reflects his/her role as CEO or is a personal outlet. (*See section below regarding employee use of social media.*) An example of this is the resignation of former Sun Microsystems CEO Jonathan Schwartz, who used Twitter.[244]

Potential issues under U.S. law

Does your Human Resources Department use social media as a recruiting tool? Do they use it to investigate the credentials and qualifications of job applicants? Is it used to track the activities of current employees? If so, be sensitive and current on possible privacy rights, compliance with the federal Fair Credit Reporting Act, the National Labor Relations Act ("NLRA"), the federal Electronic

Communications Privacy Act, Title VII, and state laws that outlaw adverse employment action for off-site actions by employees that are not unlawful, such as smoking.

An employer may also use social media to ferret out fraudulent medical (including Family Medical Leave Act) claims. Insurance carriers and employers are increasingly using social media sites to expose claimants supposedly too injured to work, but boastful of their physical prowess on their personal sites.[245]

Social networking sites have unlocked countless electronic doors for employers to learn about employees. While employees can be and are "themselves" on one site and anonymous or disguised on others, employers act at their legal peril to pretend to be "someone else" when monitoring employees and applicants. There are a number of ways an employer may obtain an employee's actual or implied consent to monitor her/his off duty social networking. But an employer must always act with integrity, because courts have held "disguised" employers liable for pretending to gain access to employee-created social networking groups.

In addition, even with consent to monitor, only seek work-related information. An employer must take steps to avoid obtaining more information than required to make an employment decision. Information to avoid includes an employee's membership in a protected class, a lawful association such as a union, or in legal political activities.

Even where there is no unionized workforce present, communications between employees that discuss efforts to organize, or engage in conduct that is protected under section 7 of the NLRA, may not impose policies that unlawfully interfere with the employees' exercise of those rights. Employers must also refrain from monitoring what is lawful communication between employees regarding unionization or union business to avoid charges of surveillance, which also violates the NLRA.

Public employers must, as with all practices, observe due process rights of employees with respect to conducting searches and any resulting disciplinary action. The mere fact that the conduct occurs on the Internet does make the conduct either protected or unprotected; rather, the context in which the conduct occurs—such as is it a comment posted by the employee, is it accessible on a public site or page, what issues the comment addresses—must be considered.

Finally, and particularly in privacy-type cases, courts and juries are easily offended and punish employers that use more intrusive methods over other available, less intrusive alternatives.

Potential issues under English law

Employers in the UK face similar issues in relation to the use of social media as part of the application and vetting process. An employer's use of a job applicant's data, which is available on the Internet through social media, is governed by the Data Protection Act 1998 (the "DPA"). The DPA requires an employer to obtain an applicant's consent for the collection and use of such data to be used as part of an application or vetting process.[246] In addition to data protection issues, exploring information relating to a job applicant that is available on the Internet through social media may expose the employer to claims of discrimination if the employer decides not to proceed with that applicant (regardless of the employer's actual reasons for choosing not to do so). For example, there could be such an exposure where the data available through social media gives information as to an applicant's race, colour, religious beliefs or sexual orientation that might not otherwise be apparent through the application process. Employers should therefore consider whether the benefits of obtaining information through social media outweigh the risks of potential litigation.

The use of information available through social media to investigate possible employee misconduct or breaches of an employment contract also gives rise to potential issues. It is unlikely that employees or workers will provide consent for employers to comb through information that is available through social media. Accordingly, the employer's interest in searching for and using such information in the absence of employee or worker consent must be carefully balanced against (and be shown to outweigh) any detriment to the employee or worker in order for the use of such information not to breach the DPA or any rights of privacy that the employee or worker may have.[247]

Employers should therefore consider including, as a standard contract term, a provision by which the employee gives consent. Employers should also have a clear and well-publicised policymaking that establishes that such information would be used in the event of an investigation as a step toward demonstrating that such an interest does exist. Employers should also refrain from searching and using information available through social media until a reasonable belief of wrongdoing has been established through less intrusive means of investigation.

Dismissals of employees that are based on information obtained in breach of the DPA or that unreasonably infringe upon an employee's home or private life may be found by

an Employment Tribunal to be unfair. Such dismissals may also be found to constitute an unreasonable breach of the ACAS Code of Practice on Disciplinary and Grievance matters, which may result in any award of compensation made to an employee by an Employment Tribunal being increased by up to 25 percent.[248]

Potential issues under French law

In recruiting new employees, employers should proceed with caution in seeking information available on applicants through social media, because this could be risky on a number of counts.

In particular, such a practice could be in breach of the strict rules laid down in the French Labour Code regarding recruitment methods, which state, for example, that information requested of an applicant must have a direct link with either the job opening in question or the candidate's professional capabilities. In addition, the Works Council is to be kept informed of recruitment methods and techniques.[249]

While it may be difficult to establish an employer breach of these regulations by vetting candidates through the Internet, the risk of unlawful discrimination (based on union membership, race, etc.), remains significant. While relatively few complaints are actually brought before tribunals concerning the recruitment procedure[250], such actions have multiplied over the past few years through the work of the HALDE[251], the official body acting for equal opportunities. Arguably more destructive to companies than actual litigation is the damage to their reputation when doubtful and discriminatory recruitment practices are alleged by this organization[252].

Another administrative body publishing guidelines and monitoring the use of social media, especially by recruitment agencies, is the data protection agency, the CNIL.[253] Its 2009 report included warnings against excessive and illegal acts by employers when utilising social media in the recruitment process, particularly by invasions of privacy and illegal discrimination.

In this context, a number of professional organizations, recruitment agencies and companies[254] composed a Charter on social media in which the signatories shall not use social networks to collect personal information on applicants[255].

A central question in employer use of social media in investigating the behaviour of existing employees concerns the admissibility of evidence. As in the United States, the mere fact that employee conduct occurs on the Internet does not determine whether it is protected. Instead, such protection should depend rather on the extent to which the page containing the comment can be accessed by others.

In a pending case before the Labour Court, judges will rule on whether a comment posted by an employee connected from home on his personal Facebook page should be considered as private correspondence.[256]

Unlike the suggested solution in the UK, however, an employee's agreement in advance to permit online monitoring of his or her activity by the employer is likely to be held null and void in France because both the Labour code and the courts are very protective of employee civil liberties such as freedom of expression and the respect of private life.

Moreover, unlike the United States, employees are generally immune from discipline and other sanctions for off-duty lawful (nor even unlawful) conduct. But we expect the omnipresence and ever-increasing use of new technologies for professional and personal use will undoubtedly test such "hands off" limits.

Employee Use of Social Media

Potential issues under U.S. law

Do any or many of your employees have or contribute to social media pages or spaces? If so, do they visit them at work? During working hours? Using company equipment? The answer to each question is likely yes. Facebook alone boasts more than 400 million users. A 2009 Deloitte survey revealed that 55 percent of all employees visit social networking sites at least weekly, with 15 percent admitting access for personal reasons from work.[257]. In such situations, an employer can and should lawfully restrict an employee's use of social media within reasonable limits at work, and on break-time if it impacts anyone's work adversely. A properly worded notice to employees provides an employer with a strong right to control the use of its own property, such as computers, cell phones, and PDAs. Similarly, again with proper notice, employers may also monitor the use of the company's property without restriction.[258]

An employee's "on-the-clock" time belongs to the employer, and it therefore can and should 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 personal use, unless, as stated, it adversely

impacts the workplace, either by reduced productivity or by conduct that may expose the employer to liability. At least one court has held that an employer has a duty to remedy co-employee harassment to avoid a hostile work environment, when its male employees used a company bulletin board to harass a female employee based upon her sex and in retaliation for her filing a lawsuit.[259]

Social media sites can be, and are often, used as communication tools between employees. However, at times, these employee communications cross the line into harassing, threatening, or other unlawful conduct, or divulging trade secrets or other confidential information about the employer or a competitor. In such a situation, whether an employer may be held legally liable for damages resulting from the offending employee's post, remains in gestation.[260]

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. Content posted anonymously is, of course, exceedingly difficult to police, and several state laws prohibit employers from taking adverse action against an employee for engaging in lawful, off-duty conduct, including political activity or affiliations specifically protected under state law. Moreover, employers must be cautious about taking adverse action against an employee whose social media use could be protected under the NLRA or federal and state whistleblower laws, such as the Sarbanes-Oxley Act. Finally, "public" (meaning government) employers have the additional burden of avoiding any violation of their employees' First Amendment and other Bill of Rights protections by disciplining them for content posted on a social media site.

On the other hand, employers cannot "play ostrich" to employee abuse of social media sites. Consequences of doing so include loss of confidential information and/or trade secrets; irreparable damage to reputation or other aspects of a business, either through employee misconduct or apparent company condonation or endorsement by inaction; or liability for employee content that is defamatory, threatening or otherwise unlawful. Employers also have a duty to report illegal activities to the proper authorities and to take internal action when it becomes aware than an employee has engaged in unlawful activity.[261] Recently, the FTC revised the Guides Concerning the Use of Endorsements and Testimonials in Advertising.[262] It is unclear to what extent, if any, an employer may be liable for an employee's statements in social media; but the FTC provides an 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. Unknown 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.

Potential issues under English law

Employers based in the UK may also lawfully restrict employees' use of social media through the employer's equipment. A properly worded and well-publicised policy would be key to achieving this objective and would ideally be coupled with the use of technological means to prevent employee access to social media using employer equipment, either absolutely or for certain periods of the day.

Where an employer lacks technical means to prevent access to social media through its equipment, an employer may consider monitoring to detect any breaches of its policy (any such policy needs to provide employees with clear guidance as to the levels of use permitted – if any). Employers in the UK do not have an absolute right to monitor employees' use of the employer's electronic equipment, and the more intrusive and/or secretive any monitoring is, the more likely it would be that such monitoring would be unlawful.[263] Accordingly, employers may consider using spot checks rather than ongoing monitoring, and setting flags so that any monitoring just returns details as to when social media websites are accessed, rather than monitoring the actual content viewed or submitted. If it becomes relevant to consider the content viewed, it is more likely to be lawful for an employer to do so as part of an investigation that is triggered by less intrusive monitoring.

Where employees use their own equipment, such as their personal mobile phones, to access social media, the position is the same as applies in the United States.[264] The UK employer cannot monitor electronically, but may investigate and, if necessary, implement disciplinary

proceedings if there are productivity or other performance or conduct issues, or if employees use social media through their own equipment to act unlawfully – for example, by behaving inappropriately toward co-workers.

As is the case in the United States, it is an open question whether an employer may be liable for an employee's use of social media that discriminates against or harasses or threatens a co-worker. An employer is, generally, vicariously liable for an act of harassment or other discrimination carried out by an employee during the course of their employment.[265] Whether or not harassment carried out via social media would be capable of falling into this category is currently undecided. It is more likely that the employer would be vicariously liable for an employee's use of social media if the employee in question is a manager who publishes something inappropriate concerning one of the persons for whom that manager is responsible. Whether any such misuse occurs during or after working hours or on the employer's equipment may also be factors as to whether the employer should be vicariously liable.

Whether content published by or about an employee can provide the basis for disciplinary proceedings will depend largely upon the circumstances. For example, was the content published during or after working hours? Did the employee disclose confidential information of the employer? Did the employee use the employer's or the employee's own equipment to publish the content? Does the content constitute inappropriate behaviour toward a co-worker and, if so, can publishing the content be linked to the employee's professional (as opposed to private) relationship with that co-worker? Does the content, such as a status update, indicate that the employee has been untruthful toward their employer (for, example showing the employee to be well and active when the employee has informed the employer that they are unfit to attend for work)?[266] As with monitoring, it is important that the employer has come to collect and use any such content with regard to the DPA and any privacy rights that the employee may have.

Caution should be exercised before taking any adverse action against an employee who publishes content that raises a complaint against the employer. Whilst the inappropriate publishing of any such information needs to be dealt with, the employer should also investigate the substance of the complaint made by the employee. Content might conceivably be published in such a way as to constitute a written grievance (which a failure to deal with through the grievance process may expose the employer to an increase in compensation of up to 25 percent where the employee brings a successful complaint before the Employment Tribunal).

Potential issues under French law

As in the UK, employers may technically impede employee access to social media sites from their own computers, cell phones and PDAs.

They may also lawfully restrict employee use of social media at work by specifying such restrictions in a specific document related to the use of information technologies, a *"charte informatique."* In this case, employers would need to monitor employee use of social media (websites visited and length of the visits)[267], given the liability they incur regarding IT security issues and the behaviour of their employees on the Internet.

In both cases, the employer must comply with a very formal procedure, which includes informing the employees, consulting staff representatives and completing a declaration to the CNIL[268], given the personal data which will automatically be collected in this process.

However, in cases of co-employee harassment, the French employer cannot be too careful. Even such close monitoring of Internet activity would occur too late to release the employer from its liability. Indeed, according to French case law, employers have a duty to prevent co-employee harassment from occurring in the first place[269]. The employer would therefore be liable where co-employee harassment occurs, even if he had taken measures to detect the "electronic" harasser and to protect the victim (by dismissing the perpetrator).

Nevertheless, it could always be put forward as evidence of the employer's good faith in case of litigation, that the employer had included in the aforementioned *"charte informatique"* clear prohibition of any harassment or similar behaviour through social media.

Removing Content Posted by Employees from the Site

If an employee posts derogatory, defamatory, harassing, threatening, confidential or other unlawful or inappropriate content, what can and should the company do to remove the content from the social media site?

Most social media sites have terms of use that prohibit the posting of any content that 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.[270] Not all sites, however, 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."[271] 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."[272]

If, for instance, an employer complains to Facebook that a post discloses confidential information pertaining to the company, but fails to prove that the information is legally protected, Facebook may not remove the offending post. Indeed, currently, no laws *require* Facebook to remove such a post.

In the UK, a further step that might be considered is to ask the employee concerned to remove any offending content. If the employee refuses to do so, it may, depending on the content, be possible to bring a disciplinary action against the employee for refusing to follow a reasonable and lawful order.

Current Legal and Regulatory Framework in Employment

Little case law exists in the United States or the UK pertaining to employee use or abuse of social media, and no statutes or regulations 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.

In the United States

An employer can and should always prohibit employees from posting anything that amounts to unlawful harassment or discrimination. Title VII of the Civil Rights Act of 1964 and its amendments[273], as well as numerous state laws, prohibit harassment of employees by other employees based on certain protected characteristics. What conduct constitutes harassment based on a protected characteristic and whether such conduct is sufficiently severe or pervasive to be unlawful are often difficult to unravel. To further complicate the issue, and to reiterate, several states prohibit employers from taking adverse action against an employee for engaging in lawful, off-duty conduct.[274] It is therefore unclear in some states 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, case law is still unclear on what, if any, circumstances expose an employer to vicarious liability for an employee's alleged harassment of another on a social media site. One court recently held that an employer was not liable for an employee who used his company phone and computer to harass non-employees. Another dismissed a negative supervision claim because it was not reasonably foreseeable that unsupervised Internet access would result in harm to others. In another decision, the same court held that an employer is only required to prevent foreseeable on-the-job misconduct, not to supervise an employee's private conduct or persistently scan the World Wide Web to ferret out potential employee misconduct. [275] 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.[276] However, because 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.

Other examples of where an employer must use caution are 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[277], or where the disciplinary actions may be illegal retaliation under a host of federal, state, and local anti-retaliation statutory provisions. Under the NLRA, for instance, an employee may be free to express his/her opinion on working conditions, even if it is derogatory to the company and/or other employees. Employee privacy rights may also play a role, depending upon how the employer became aware of the offending conduct. Finally, to repeat,

government employers must consider their employees' First Amendment and similar rights if the scope of the prohibited use of social media arguably affects an employee's right to speak on an issue of public concern.

In the UK

Because of discrimination legislation and other contractual and statutory obligations upon employers to protect employees from harassment, employers can prohibit employees from posting content that bullies, harasses or discriminates against their co-workers. However, the boundaries of these protections have not yet been tested fully before the Employment Tribunal and, as indicated above, there are a number of open questions as to the circumstances in which an employer can take action against an employee who behaves inappropriately toward a co-worker through social media.

In France

As in the United States and the UK, there are neither statutes nor regulations specifically governing employee use of social media.

The first employment law rulings on questions of social media in the workplace are eagerly awaited, particularly as regards the courts' treatment of the issue of whether evidence collected through social media is admissible.

However, there is some recent case law in related areas (dealing with issues such as new technologies, monitoring of employee behavior and data protection) that may provide us with clues on the position of the French Supreme Court[278], as regards the importance of the protection of employee civil liberties when faced with the interests, rights and obligations of entrepreneurs.

For example, the first Supreme Court decision on the Sarbanes Oxley whistleblowing obligations was rendered in December 2009 to a frenzy of media attention. In this case, involving a leading French software company, the whistleblowing policy was contained within a Code of Conduct that also included rules on the use of information classed both as confidential and also "for internal use." The chapter on whistleblowing was held as being in violation of data-protection laws and as not providing enough protection to employees, whilst the rules on the treatment of information "for internal use" were held to be in breach of freedom of expression and of a separate collective right of expression enjoyed by employees with regard to their working conditions[279].

Another trial court case on whistleblowing held that the facility to denounce delinquent conduct through an intranet site did not sufficiently protect employee rights, as proper procedure as regards the staff representatives had not been respected and the examples of targeted behavior were much wider than those aimed at by the Sarbanes Oxley legislation[280].

Finally, case law surrounding blogging and online communication by trade unions and staff representatives or employees in contentious situations with their employer usually considers the level of public access to the chosen media, as well as the content and the context of the publications in order to reconcile the conflicting rights and interests of the concerned parties.

Social media and its associated advantages and risks are now inextricably linked with other topical HR subjects, such as stress and psychosocial risks, harassment, discrimination and diversity, the growing status of the CHSCT (Health and Safety at Work Committee), etc. For these reasons alone, Social Media cannot be ignored. Employers must consider developments in these other areas and factor such considerations into the drawing up or revision of company policies and handbooks, IT charters, codes of ethics, etc. Finally, when considering the drafting and implementation of any such documents, French employers must pay attention to possible procedural obligations in terms of staff representatives, as well as guidelines and regulations set down by organisations such as the HALDE and the CNIL.

Bottom Line—What You Need To Do

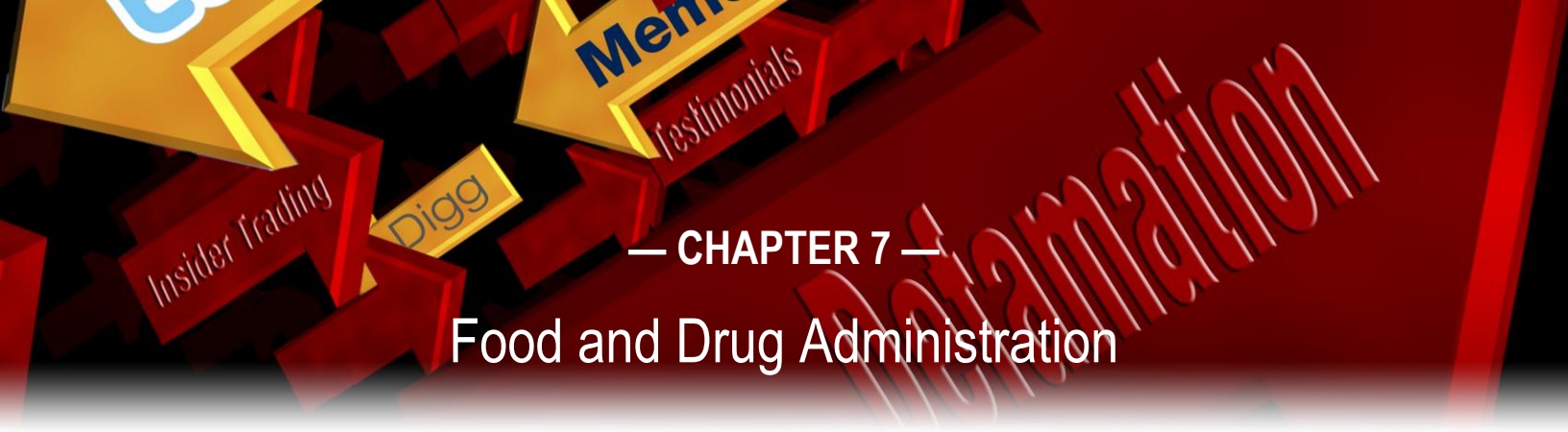
If your company has not developed policies for use of social media by your employees, do it now. A properly drafted and enforced policy on the use of social media by employees is an employer's most effective tool in protecting itself against legal liability and harm to its reputation, and good will from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

In most cases, a properly drafted policy pertaining to employee use of social media will assist an employer in protecting its interests and guiding employees on acceptable and unacceptable online behaviour. 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) stressing the ownership and ability to monitor the company computer system(s) and related equipment, and explaining that no duty of privacy can be expected with the usage of these systems; (2) the company's level of tolerance for personal use of social media; (3) whether the company should permit or even require use of social media for marketing and business development; (4) how the company will handle employees who post arguably inappropriate, but not unlawful, posts such as illicit photos, profanity or other potentially derogatory content; (5) how the company will comply with laws protecting employees' rights to engage in lawful off-duty conduct, but still ensure nothing damaging is posted online; (6) how the company will train employees, once the policy is in place, so they understand what is forbidden (for example, one person's definition of "crude" may vary from another's); (7) how the company will monitor compliance with and enforce the policy; (8) what the repercussions will be for violations; and (9) keeping the policy simple and reactive to ever-morphing social media.

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



— CHAPTER 7 —

Food and Drug Administration

Chapter Authors[281]

Colleen T. Davies, Partner – cdavies@reedsmith.com

Kevin M. Madagan, Associate – kmadagan@reedsmith.com

Introduction

Social media, the now-entrenched Internet phenomenon, enables decentralized, real-time communication among small and large groups of individuals, organizations and businesses. Social media is a fast-paced, immediately gratifying interactive communication venue that allows website content to evolve and be transmitted instantaneously to an audience of anonymous, active or passive observers.

The ability to communicate so fluidly, however, renders social media communications reliably *unpredictable* and *illusive*, thus posing unique challenges for regulatory authorities as well as the companies they regulate, especially with regard to advertising. One of those regulatory authorities, the Food and Drug Administration ("FDA"), has jurisdiction over companies involved with the manufacturing of medical products, such as drugs, biologics, medical devices, and emerging biotechnology products.

This chapter explains why even though various business sectors have fervently embraced social media as a product marketing tool, the FDA-regulated industry has been slow to adopt this practice. It also explores FDA's emerging policy on Internet marketing activities, and specifically the potential risks associated with using social media to disseminate promotional messages and scientific information about FDA-regulated prescription drugs and devices. It then provides suggestions on how to proceed now, before FDA issues a guidance document on social media and product promotion.

Social Media in Action in FDA-Regulated Industry

Everybody's Talking But the Experts

Conversations through online social media communities among health care professionals, consumers, and others, about FDA-regulated prescription products and disease-states have been taking place for some time. Sermo, for example, one of the largest online physician social networks spanning 68 specialties in 50 states, was launched in 2006 and now provides a venue for more than 112,000 physicians to exchange observations in real-time about drugs, devices and clinical issues. Consumers are equally active. More than 60 million consumers used social media to communicate and research health and medical information in 2008.[282]

What is lacking in many of these social media communications, however, is an authoritative source of information about prescription products and the conditions and diseases for which they are used. As experts on their products, many companies want to serve in this capacity. They want to use social media to disseminate information about their products to ensure that accurate, transparent, high-quality information is being communicated to social media participants. Many feel this could be one of the best ways to reach target audiences effectively.

But companies are concerned about the not-insignificant consequences of improper marketing, which can vary, but which may include the cost of remedial advertising, damage to reputation, and civil fines.[283] The government, for example, has collected billions of dollars in fines, forfeitures, and disgorgements from drug companies over their practice of marketing products for unapproved, or "off-label," uses.[284] In the worst case, violating the Food, Drug, and Cosmetic Act ("FDCA") may be considered a strict

liability misdemeanor, which becomes a felony when there is intent to defraud or mislead.[285]

Not surprisingly, then, without some guidance from FDA, companies are not using social media to market their prescription products. Prescription product marketing has been restricted to more controlled, non-interactive strategies using conventional Internet outlets, such as fixed websites, and links to and from websites—which, by today's standards, are antiquated avenues for advertising.

To be fair, companies are not avoiding social media entirely; many have a social media presence through company blogs, Facebook pages, YouTube channels, LinkedIn profiles, and Twitter accounts. But the information disseminated through these venues is mostly limited to information about corporate developments and health conditions or diseases. To the extent that these venues are being used to disseminate information about prescription products, such as a YouTube video, for example, the very features that make the media "social" have been disabled (*e.g.*, the ability to post comments under a YouTube video).

Current Legal and Regulatory Framework

FDA's Emerging Social Media Policy

FDA's rules were written long, long before the Internet was even a word. They contemplate large, cohesive swaths of information, uninterrupted by others' comments, reactions, or discussion, and require careful attention to ensure that promotional messages are truthful, non-misleading, and fairly balanced between the benefits and risks associated with a particular product.[286] When these regulations are applied to any activity on the Internet, determining what is promotional and how to apply the regulations can be challenging. FDA held public hearings on Internet advertising and promotion in 1996,[287] but then failed to issue any guidelines and subsequently halted all such work, presumably because the agency was not ready or prepared, or even knew how to act. In 1999, FDA further delayed taking a position by informing the industry that it would "look at [Internet] issues on a case-by-case basis," while reserving the right to revaluate the need for regulations in the future.[288] As a result, in order to glean FDA's Internet and social media policy, the industry has been forced to scrutinize individual enforcement actions against companies that have created and used Internet websites for improper promotion of their products.[289]

Yet, in many ways, these enforcement actions have been similar to more traditional advertising actions in that the website owner had control of the content, its display, and access to it. In 2008, for example, FDA issued a Warning Letter concerning a YouTube video advertisement, but the fact that the video was posted on YouTube was irrelevant; the Warning Letter would have been the same had the video been broadcast in a promotional conference hall.

There are some exceptions, however, including few actions that highlight challenges particular to the Internet, such as determining when a link from page-to-page or from website-to-website is a continuation of the advertisement and, thus, also subject to the many regulatory content requirements and restrictions. For instance, over the past few years, the industry had developed a theory commonly referred to as the "one-click" rule under which FDA's requirement to provide comprehensive product information, including safety information, in promotional material can be satisfied if such information is directly accessible from a link in the original promotional piece (*i.e.,* no more than one click away). This rule was placed into question when FDA issued enforcement letters last year to 14 companies for their failure to include risk information in Google banner advertisements.[290] These letters first revealed FDA's new thinking on the matter, and sent shock waves throughout the industry, causing many companies to reassess their Internet marketing strategies. FDA has subsequently stated that it "never had what some are referring to as a 'one-click rule.'"[291]

Recent Developments

Like a giant awakening from a 100-year nap, FDA recently acknowledged the special nature of the Internet as a marketing tool and venue, and has renewed its interest in addressing Internet communications. FDA held a public hearing in November 2009 and solicited written comments through a public docket that was open from September 2009 to February 2010. These actions are intended to help FDA determine how the statutory provisions, regulations, and policies concerning advertising and promotional labeling should be applied to product-related information on the Internet and newer technologies.[292] Recently, FDA made the following statement about social media and compliance:

> We believe it is a good idea for companies to have a robust policy in place for any type of promotion about their products, including social media promotion. We would advise them to carefully review their materials and processes to ensure that their promotion is compliant with the regulations. Consumers and healthcare professionals deserve an accurate and

> balanced picture of a drug product when it is promoted.
> …
>
> [FDA's advertising and promotion] rules apply regardless of the medium used.
> …
>
> * * * all promotional communications about prescription drugs that are disseminated by or on behalf of a manufacturer [must] be truthful, non-misleading and balanced.[293]

FDA recently announced that it intends to issue a guidance document in 2010 on social media and the promotion of prescription products.[294] FDA may also propose new regulations within the next year, as encouraged by many participants at the social media hearing and in written comments to FDA's social media docket.

But before doing any of these things, FDA must resolve the issues it has been avoiding over the past decade. Listed below are only a few of these issues.

Internet Control

The Internet is growing exponentially and the industry cannot monitor every Internet website or communication. The industry does not want to be held liable for content that it does not generate or encourage. For example, the industry does not want to be held accountable for social media that is posted or becomes part of a website without their permission or knowledge (*e.g.*, Google Sidewiki, a browser sidebar allows the public to contribute and read information alongside any web page without the website owner's consent). But the industry also understands that it may be liable for some content depending on its ability to influence or control the environment through which the content is communicated—the need to take corrective action, for example, could depend on whether a company controls the social media environment (*e.g.*, hosts or sponsors the environment), or is merely a participant in an environment controlled by a third party.

Transparency

FDA and industry must work together to ensure consumers have access to accurate and truthful information about FDA-regulated products by making it easier to distinguish between third-party and company controlled website content.

Space Limitations

The industry wants FDA to account for the evolving nature of social media and space constraints. Guidelines or regulations regarding dissemination of risk information should be principal-based and applicable to multiple social media formats. Despite FDA's position on the one-click rule, many in the industry have called for FDA to adopt a modified version of the rule by allowing a company to present a brief introduction of its product (*e.g.*, an abbreviated reference to the product's indication and its most significant risks) based on the space constraints of the social media itself, provided there is also easy access to full product information through a hyperlink.

Third-Party Social Media

By participating in an online discussion through social media (*e.g.*, real-time chat room), the industry is concerned that it may be held responsible for any statements made during the discussion, even by unrelated third parties. The industry is calling for FDA to permit companies to engage in online discussions without becoming responsible for all content, provided the communications are truthful, non-misleading, and in accordance with any FDA standards for providing risk information through social media. Many want FDA to provide them the freedom to determine whether and when to participate in or to correct information on third-party sites.

Off-Label Discussions

Given today's regulatory environment, where manufacturers are routinely held responsible for anything involving their products, there is trepidation that any off-label discussion or reference on an interactive social media site, even if it is a professional site for scientific exchange,[295] will impute knowledge and consent of an unapproved use to the manufacturer.[296] This knowledge requires the manufacturer to provide adequate labeling, such as adding a warning or precaution, or obtaining FDA approval for the product to be so used. Otherwise, the product may be considered misbranded and the manufacturer could be held liable for promoting an unapproved use.

For company-controlled websites, some have proposed requiring social media participants to agree to terms of use prohibiting off-label discussion. A company could then monitor the website to ensure compliance with these terms and, if necessary, take corrective action, which may include removing any off-label discussions. Liability for off-label discussions may depend on the amount of control a company has over the social media environment itself.

Yet, even if FDA issues guidance addressing off-label concerns, enforcement decisions under the FDCA are not solely FDA's province. The Department of Justice ("DOJ")

represents FDA in formal enforcement actions and does not always agree with FDA; the DOJ has a history of scrutinizing conduct that appeared consistent with FDA guidance.

2253 Submissions

FDA requires all prescription drug labeling and advertising to be submitted at the time of initial dissemination through an FDA Form 2253.[297] Because some social media communications (*e.g.*, real-time chat room discussions) are, in many regards, analogous to those taking place between company sales representatives and health care professionals or patients, many in the industry believe the Form 2253 reporting requirement for social media should be limited to some extent. FDA may decide to require companies to submit only the static elements of social media environments controlled by a company, and promotional postings on social media controlled by third parties.

Advisory Boards and Workshops

The Internet will continue to emerge at a faster pace than can be regulated by FDA's regulatory process. To address this issue, FDA could create an advisory board that would work closely with the industry through meetings and workshops to collectively leverage knowledge, expertise, and experience to generate ideas and viable solutions to problems posed by emerging technology.

Adverse Event Reporting

Adverse event reporting through social media must be addressed because adverse event reporting regulations could be interpreted in a way that would require a company to monitor the Internet and social media sites, and investigate adverse event information learned from such sites.[298] Listed below are a few issues and proposals specific to social media and adverse event reporting.

- *Adverse Event (MedWatch Icon):* The general consensus is that FDA's MedWatch icon should be posted throughout the web to facilitate adverse event reporting. Some propose requiring the icon on all industry-sponsored sites, including educational/disease websites. Others proposed allowing the icon to provide a safe harbor to companies participating in certain social media technologies (*e.g.*, blogs, chat rooms). This would allow and may even encourage the industry to contribute to important product-related dialogues currently held by consumers and professionals in social media contexts.
- *Adverse Event (Monitoring):* Although FDA could require the industry to actively monitor all Internet social media for adverse events, in light of the issues discussed earlier in this chapter about Internet growth and control, FDA more likely will require the industry to actively monitor only websites they control or influence.
- *Adverse Event (Pursuing Incomplete Adverse Event Reports):* Whether incomplete adverse event reports (*e.g.*, anonymous website postings) should be pursued, and even whether certain social media is an appropriate context for the industry to investigate potential adverse events, remains unresolved. For example, if a consumer posts a response on a discussion board about a non-specific drug treatment for a certain condition—setting aside the fact that the consumer may not be asking for assistance or reporting anything—FDA may not want to encourage the industry to post responses that could interfere with the purpose of the chat room or dialogue (a post on a third-party discussion board that does not reference a product name could generate 50 responses from manufacturers and significantly interfere with the discussion). Prior FDA guidance on adverse event reporting states that manufacturers should review any Internet sites they sponsor for adverse experience information, and they are responsible for reviewing third-party Internet sites only when they become aware of a potentially reportable issue on the site.[299] But until FDA takes a position on adverse events reported through social media, this guidance does not necessarily apply to social media.
- *Adverse Event (Trend Reporting):* FDA could encourage the use of data-mining technologies to help identify trends and patterns in patient communications about adverse events that would trigger further analysis by FDA or the industry.

Next Steps at FDA

FDA has taken its first few steps in what will likely be a long process within the agency to establish a framework for regulating the Internet, provide guidance to the industry, and find a way to adapt to emerging technologies, including social media. We have seen some encouraging signs over the past several months that FDA may be willing to adjust its current practice of attempting to apply the same standard to print and Internet communications and advertising. In his closing remarks at the 2009 hearing, Tom Abrams, Director of FDA's Division of Drug Marketing,

Advertising, and Communications ("DDMAC"), said "what we have heard is it's [the Internet] a different medium," and FDA "must get this right." We can only hope FDA is sincere in continuing to address this issue throughout 2010, and continues to engage the industry as it did during the recent public hearing.

Bottom Line—What You Need To Do To Mitigate Risk

- Until FDA issues formal guidelines or promulgates new regulations governing Internet communications, you must assume that FDA will review any social media communications through existing FDA regulations.
- Develop policies governing employee use of social media.
- Closely monitor and enforce these policies.
- Closely track FDA warning and untitled letters to avoid the mistakes your peers make when they communicate through social media.
- Participate in all FDA meetings and provide FDA with information when requested.
- Pay attention. FDA's Internet policy may emerge quickly over the next two years. There will likely be an opportunity to respond to draft guidance documents, FDA/industry hearings, and draft regulations.

— CHAPTER 8 —

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. Today, a great number of federal and state agencies utilize at least one form of social media in furtherance of their agency mission. 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.

These new platforms provide increased ability to access and interact, but 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 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.

The Department of Defense recognized that social media may be an important tool to fulfill government policies, but it must be regulated:

> On balance, DOD needs to appreciate that social software exists, is becoming increasingly popular, and has empowered people to self-organize outside government and other major institutions without permission, endorsement, or encouragement. DOD needs to be prepared to not only research, build, and/or acquire social software tools, but also to be prepared to educate its workforce about how to use them, and why.[300]

As each government agency adopts policies and guidelines for the use of social media in order to manage behaviour of government employees and interaction with the public, government contractors must understand and maintain

compliance with each agency's internal policies or face potential pitfalls associated with non-compliance. In particular, contractors who have access to government computers and information systems or sensitive and classified information will be required to establish robust compliance programs in place for security. Contractors whose employees have access to government computers or computer systems are at the greatest risk, and must take a proactive approach in ensuring employees are properly trained to protect sensitive information. Contractors who fail to address these issues may be prevented from obtaining government contracts, may find themselves in breach of security policies, or may be subject to civil or criminal liability for disclosure. Moreover, contractors without internal social media compliance programs subject themselves to the same privacy, security, and other risks associated with social media that concern the government.

In addition, companies providing social media platforms to the government must also be aware of specialized procurement and contracting regulations, and increased transparency in providing services to the government. The government has taken a close look at how procurement rules relate to companies offering social media tools to government agencies and their employees.[301] Further, government contractors who provide social media services to the government are subject to increased transparency, such as freedom of information act requests regarding their provision of services to the government. In August 2009, the Electronic Privacy Information Center ("EPIC") compelled disclosure of government contracts with Facebook, Google (YouTube), Blip.tv, Blist, Yahoo! (Flickr) and MySpace.[302] Some of the agreements allowed companies to track users of government websites for advertising purposes. Accordingly, social media providers who contract with the government must be aware of the disclosure risks of contracts from legal and public relations perspectives.

Finally, as a result of gov 2.0, government information and communications are happening faster and being shared with a wider audience. Gov 2.0 utilizes social media technologies to make networking and engagement with the public simple and powerful, make research faster, identify influencers in useful micro-niches, provide mechanisms for combating negative publicity, and measure public sentiment to help inform public policy. Government contracts similarly may utilize social media as a strategic tool to increase access and communication with the government, and influence policy and perception to better position itself to receive government contracts and grants. Government contractors can develop strategies consistent with applicable laws and policies to take advantage of gov 2.0, and use social media as a tool to their competitive advantage in interacting with the government.

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. (*See Volume 1, Chapter 8 – Litigation, Evidence and Privilege*) 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. (*See Chapter 6 – Employment*)

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 9 —

Insurance Recovery

Chapter Authors

United States:

Carolyn H. Rosenberg, Partner – crosenberg@reedsmith.com

United Kingdom:

Peter Hardy, Partner – phardy@reedsmith.com[303]

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 you or your company should 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, and, in the U.S. context, consumer class actions and securities claims.[304]

For a number of years the insurance market in both the United States and the UK has been developing policies and coverage extensions to address the increased risk caused by the developing use of technology in business. The policies have tended to be customized and modular wordings rather than off-the-shelf products, and have tended to reflect an insured's own perception of its exposure to this category of risk. Although initially the exposure was often labeled broadly as "cyber liability" and would cover many types of risk, the current common focus is on data protection and security and privacy. In this respect, the U.S. and UK insurance markets are currently at somewhat different stages of development. The mandatory notification requirements for data breaches that exist under U.S. state laws have crystallized an insurance market response. (*See Chapter 5 – Data Privacy & Security*) The U.S. market is relatively well-established, and the identification of appropriate coverage is often a board of directors-led initiative, most notably in the retail, health care and financial services sectors. The scope of protection has tended to focus on payment for the costs of compliance with mandatory notification requirements, defense costs (including defending or responding to any regulatory intervention), and the settlement costs of claims resulting from a breach. By adopting a modular approach to policy wording, an insured can play an active part in identifying the risk exposure of its own business and market sector and negotiating policy wording and coverage tailored to its needs. As a general observation, however, businesses that are particularly exposed to website content contamination and risks of defamation and copyright infringement are carefully scrutinized by underwriters.

In the UK and outside of the United States in general, the insurance market is less established for data protection and security and privacy coverage, not least because of the reduced scope of mandatory reporting. But the UK and European landscape is changing and moving closer to the U.S. model. Also, many businesses have a global reach that will require a risk assessment across a number of jurisdictions, including the United States. Although it is not always true that the UK insurance market follows the lead of the United States, there are obvious precedents, particularly in the area of directors' and officers' liability insurance ("D&O"), which demonstrate how this risk

category might be expected to develop in Europe in the near future. The UK is currently witnessing greater regulatory activity, and the retail and financial institutions sectors in particular are starting to develop the claims history that is often necessary before the value of the coverage is fully understood. In addition, the telecommunications industry and Internet service providers will have to adapt to being measured by new standards of reporting.

The U.S. market has established itself over the past four years in particular, and international insurance brokers, who have a presence on both sides of the Atlantic, are seeing the lessons learned being applied for the benefit of an emerging UK and European market. Data protection and security and privacy coverage is available from established carriers, and an insured would be well advised to discuss with its brokers and insurance coverage counsel the particular exposure to "cyber" and technology risks generally, and data protection and privacy rules specifically, in order to ensure that any coverage purchased is properly customized to the insured's business. This is not a sector of the insurance market where the products are sufficiently commoditized for an insured to consider an "off the shelf" purchase.

When considering purchasing or renewing insurance coverage, the steps outlined below may be helpful.

Identify Current Policies That May Provide Coverage

Companies in both the United States and the UK traditionally purchase a number of different types of insurance policies to protect themselves from exposure to claims made against the company and its management. These policies would typically include D&O liability, professional liability ("E&O"), comprehensive general liability ("CGL") (for U.S. insureds), property damage and business interruption coverage, fidelity bond policies (which are required by regulation in some industries) and fiduciary liability policies. They may also have employment practices liability ("EPL") and, as noted above, "cyber liability" and, most recently, data privacy and security liability insurance. Because 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—reviewing the 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 and losses arising from data protection issues and privacy laws will continue to grow.[305]

For example, a CGL policy issued in the United States typically provides coverage for bodily injury and property damage, as well as for advertising and personal injury. But the language should be examined to determine if there are terms, conditions or exclusions that limit or expand coverage. 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, or that are defamatory or disparaging. Although whether and how these coverages may apply depends on the language of the policy, the facts and applicable law. An insured company with business exposure in both the United States and the UK should further review the policy language to ensure that definitions and exclusions do not potentially suggest different meanings in each jurisdiction, while at the same time respecting any legal and regulatory differences that may exist. Insurance policy wording should be negotiated with an eye toward analyzing potential "buckets" for coverage should a claim be made. Similarly, a defamation claim may become an employment-related claim, and thus 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 a claim hits.

Consider New Products and Recognize They are Also Negotiable

As discussed above, cyber liability and Internet-related liability policies were introduced to the market several years ago, particularly in the United States. 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 a number of exclusions that threatened to engulf the coverage provided. The policies have improved, however, as more insurers have entered the market, as claims have matured, and as underwriters have become more comfortable with underwriting the risks. Policyholders willing to invest in reviewing and comparing choices and policy wording may be able to 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 also include regulatory actions, lawsuits, and demands. Further, coverage may 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, and civil, criminal, and administrative and regulatory proceedings. Keep in mind that a broader definition of "claim" also means a corresponding broader 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. Exclusions for bad conduct committed by insureds or employees should be triggered only by a final adjudication of the excluded conduct. Further, 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 liability coverage for claims as a result of potential breaches of security and access to private data; CGL (in the United States) 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 (and in some cases may require) reporting of potential 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, 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, depending on the coverage defenses raised by the insurer and applicable law.

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.

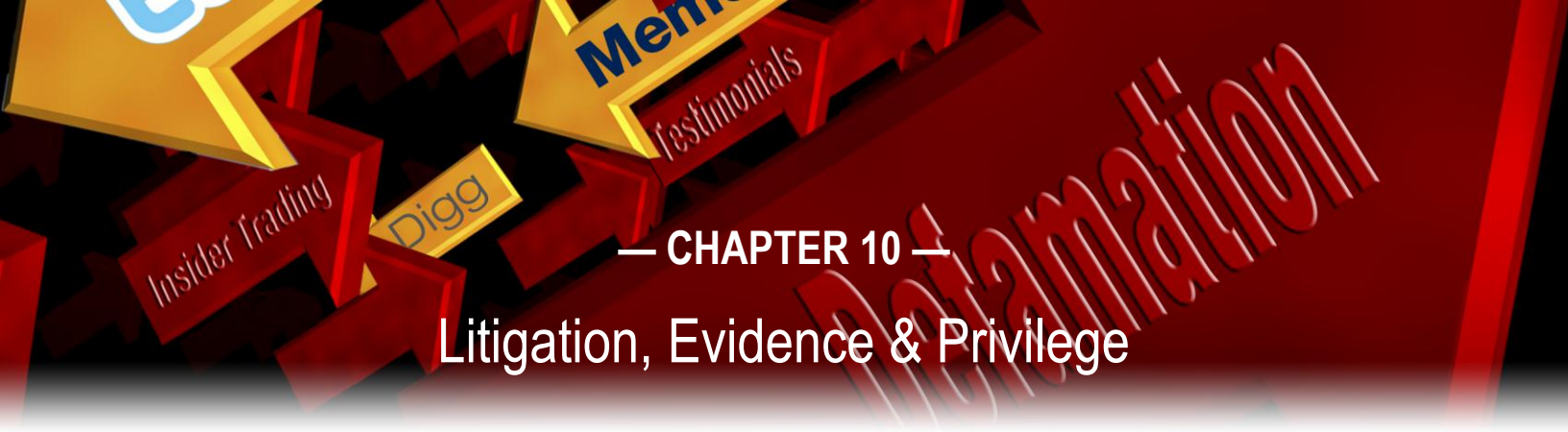
Obtain Consent to Settlement or Payment of Judgment. Know your rights and obligations. Insureds should check for any "hammer" provisions, which may limit the insured's recovery if the insured refuses to settle where the insurer is able to resolve the underlying claim. Conversely, where the insured desires 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 different provisions for resolving disputes than the primary policy(ies), making resolution of a major claim potentially challenging. It is not that unusual for an insured seeking to recover a large loss from a "tower" of insurance coverage to litigate separately in the United States and the UK (or other jurisdictions), and commence both litigation and arbitration or mediation proceedings. 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 both insurance brokers and coverage counsel, because insurance applications and the documents attached to them 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 10 —

Litigation, Evidence & Privilege

Chapter Authors[306]

United States:

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

United Kingdom:

Emma Lenthall, Partner – elenthall@reedsmith.com

Louise Berg, Associate – lberg@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, BlackBerrys, 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 realise that such postings often become a permanent record, even if the items are removed.[307]

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 which 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, expose juror misconduct, and serve legal documents. 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 its ultimate effect on business operations and public relations. (*See Chapter 6 – 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.[308]

- 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 the 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 the 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 the 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.[309]

- In *Mai-Trang Thi Nguyen v. Starbucks Coffee Corp.*, 2009 WL 4730899 (N.D. Cal. 2009), a Starbucks employee was fired for inappropriate conduct and threatening violence to fellow employees. The employee then sued Starbucks for, inter alia, sexual harassment, religious discrimination, and retaliation. The employee's MySpace page was submitted as evidence by Starbucks, where plaintiff stated: "Starbucks is in deep s**t with GOD!!! …I will now have 2 to turn 2 my revenge side (GOD'S REVENGE SIDE) 2 teach da world a lesson about stepping on GOD. I thank GOD 4 pot 2 calm down my frustrations and worries or else I will go beserk and shoot everyone…." Based on the evidence submitted by Starbucks, the court granted summary judgment in its favor.

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 6 – 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 (or the foreign equivalents) 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 to 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 realise 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 postings 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.[310]

- 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."[311]

- 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.[312]

- In December 2009, Baltimore Mayor Sheila Dixon was convicted by a jury of embezzlement for stealing gift cards intended for the less fortunate. After the verdict, her lawyers initially asked for a new trial in part because five of the jurors were communicating among themselves on Facebook during the deliberation period, and at least one of them received an outsider's online opinion regarding how the jury should decide the case.

- In an English case in November 2008, three men were on trial for child abduction and sexual assault. One juror posted details of the trial on Facebook and created a poll, stating that she did not know "which way to go." No privacy settings were activated so the

posts could be read by all other Facebook members. The juror was subsequently dismissed from the jury.

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 teams to research the social media sites during the trial to ensure that no juror is leaking the jurors' thought processes about the case to the public and/or being tainted by other individual's responses to any postings on the social media sites.

The Impact of Social Media on Methods of Service

Recent cases have also demonstrated that social media is forcing lawyers to consider more modern, and in some cases more appropriate, methods of service.

In October 2009, the English High Courts permitted service of an injunction via Twitter. In this case, which has become known as the 'Blaney's Blarney' case, an anonymous Twitter user created a profile impersonating a right-wing political commentator and solicitor, Donal Blaney. The profile posted photographs and linked to Mr Blaney's blog. Mr Blaney applied to the courts for injunctive relief against the unknown user.

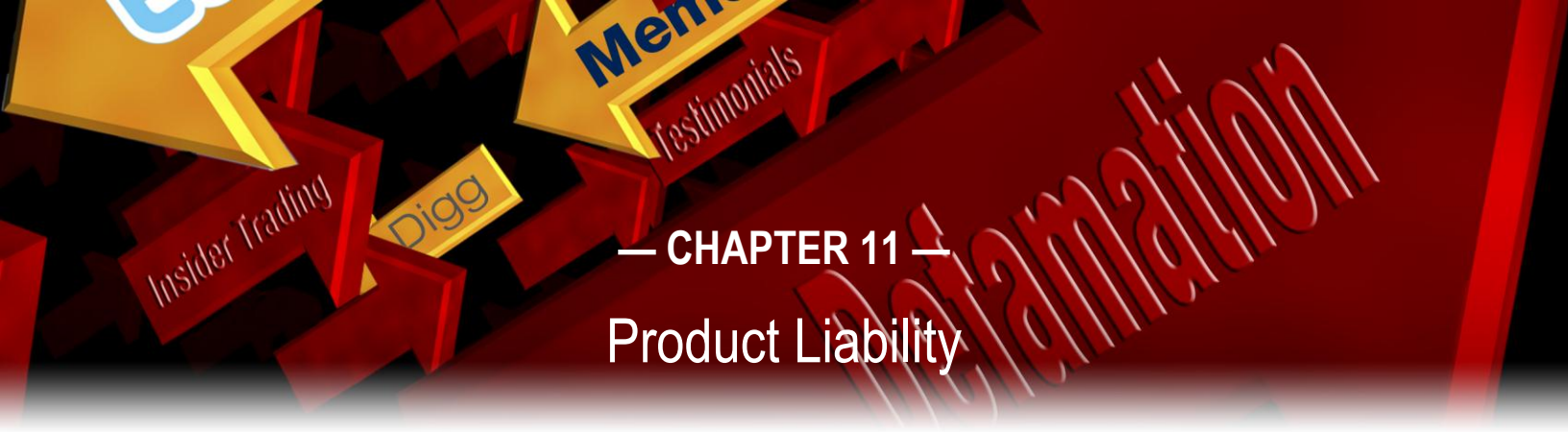
The English Civil Procedure Rules allow service by several traditional methods, but also allow a claimant to request alternative service by less conventional means. The claimant must show that there is a good reason for doing so. In this case, it was permitted on the basis that the defendant was anonymous and could not be contacted.

The English courts were shown the way by the Australian courts in 2006, when service of a default judgment was permitted via Facebook (*MKM Capital v. Corbo and Poyser*, 2008, unreported). The claimant demonstrated that all alternatives had been exhausted, as the defendants were entirely uncooperative and, although not anonymous, had provided no address. The judge also required the claimant to show that it could reasonably be assumed that the Facebook accounts were set up and maintained by the defendants – the claimant did so by matching email addresses and dates of birth, as well as showing that the defendants were 'friends'. A similar case occurred in New Zealand in March 2009.

As social media provides increasing scope for defamation and copyright infringement, more claimants likely will opt for service via these websites to overcome the obstacle of identifying the defendant. The flaw, however, in allowing such alternative methods of service may be in enforcement. In the Blaney's Blarney case, the user complied and removed the profile. Otherwise, Mr Blaney would have had to go to Twitter to obtain the user's details, and as they are based in California, there could have been problems enforcing any order.

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, in the court of public opinion, and ultimately in 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 so as to prevent such postings from undermining your company's legal position, business relations, and public image.



— CHAPTER 11 —

Product Liability

Chapter Authors[313]

United States:

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

United Kingdom:

Paul Llewellyn, Partner – pllewellyn@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, utilise 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 accessibility to information may also create problems. For product developers and manufacturers there is always a risk of legal action regarding the safety of their products. The use of social media may compound this risk by leading to (1) new legal claims and increased exposure to damages, and (2) weakened defences 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, for example, through the EC Medical Devices Directive. 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. [314] 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 potential causes-of-action under strict liability and negligence.[315] (*See Chapter 7 – FDA*) 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 contain language outside the parameters of information that the company is allowed to relay regarding its products.[316]

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 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 cannot.

One cause of action stemming from such improvident statements or omissions is a claim for negligent misstatement.

An effective claimant's lawyer is always looking for documents that show a company "puffing" or over-extolling the efficacy and safety of its products. Of great assistance to a claimant's lawyer are documents that show a company making efficacy and safety claims about its products that

are not entirely consistent with the company's "confidential" internal documents or published material. When these inconsistencies arise—particularly when a company's marketing department is not working closely enough with legal and risk management—the claimant lawyer is not only well-positioned to advance a relevant claim, but is also able to embarrass the company by asserting that it puts the company profits over safety and misleads patients and doctors, or simply 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, claimant lawyers may be able to convince a court that a company "ghost writes" information. "Ghost writing" articles or promotion materials takes place when 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 underhand and less sound than objective research in the eyes of the public. Where a company sponsors a site and has the ability to change content, the claimant will advance a "ghost writing" argument if litigation ensues, in an attempt to persuade the court that the company did not have the public's best interests in mind. Similarly, using editorial rights to silence views critical of the company's products—or favouring a competitor—would provide further arguments for a claimant lawyer. In addition, "ghost writing" can lead to unwanted, negative media attention for any company that is accused of using ghostwritten material for its benefit.[317]

If successful at portraying a company as a bad corporate actor, the claimant lawyer inevitably has an easier time proving all elements of a product liability claim (liability and causation), and positioning him or herself to secure damages award.

Bottom Line—What You Need To Do

By its very nature, social media often begets informal dialogue that is broadcast more widely than the 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). Failure to do so can result in heightened exposure to legal claims, large damages, and weakened defences.

Bottom Line—What You Need to Do

Social media implications and applications to advertising and marketing cannot be ignored; where the consumers are, and where consumers go, marketing budget ultimately follows. 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 User-Generated Content. It is critical, however, that companies do not simply adopt someone else's form. Each social media policy should be carefully considered and should address the goals and strategic initiatives of the company, and should take into account industry and business specific considerations.

— CHAPTER 12 —

Securities (UK)

Chapter Authors

Michael J. Young, Partner – myoung@reedsmith.com

James Boulton, Associate – jboulton@reedsmith.com

Introduction

This section examines the law relating to securities and investments, and how that impacts on the use of social media sites on the internet. With more than 18 million households (70 percent) in the United Kingdom having access to the Internet and more than 37.4 million (76 percent) of the adult population in the UK having accessed the Internet, legislation has had to keep pace with the emergence of new technologies and new forms of communication.

Company law has enshrined the use of the electronic communications via the Internet for a decade, and legislation regulating the promotion of financial products was introduced on a media-neutral basis in order to capture new technologies.

The Financial Services Authority (the "FSA") has also embraced the use of new technology, with a separate section of the FSA website "Moneymadeclear" providing both consumer advice on financial products and protecting against fraud such as identity theft and "boiler room" scams. Moneymadeclear also has its own Twitter feed.

We look at the dissemination of information to the public through electronic means. We also consider the financial-promotion regime in the United Kingdom and its impact on the use of social media. Finally, we examine the market-abuse regime in the United Kingdom and its relationship with the use of social media.

Dissemination of Information and Use of Electronic Communications

The use of electronic means to disseminate information to investors and the public has been enshrined in English law ever since 2000. Section 8 of the Electronic Communications Act 2000 allowed ministers to amend existing legislation to allow the use of electronic communications and storage.

The Companies Act 1985 (the "1985 Act") allowed companies to produce annual reports and annual accounts electronically and to accept proxy nomination by electronic communications, provided that the recipient had agreed to be provided with the documents either electronically or on a website.

There was also a change to the filing regime with the Registrar of Companies (Companies House) for England and Wales, as existing legislation was amended to allow for the incorporation of companies to be undertaken electronically and for certain documentation to be filed electronically.

The 1985 Act has now been repealed and has been replaced by the Companies Act 2006 (the "2006 Act"). The provisions of the 2006 Act relating to the use of the Internet came into force in January 2007.

The 2006 Act allows shareholders to communicate with a company by electronic means where the company had provided an electronic address in a notice to call a meeting or in an instrument of proxy. Schedule 5 of the 2006 Act also allows companies to send documents to shareholders in electronic form, thus removing the need to send paper copies (unless the shareholder requests a hard copy).

The 2006 Act introduced the concept of sending documents in electronic form by electronic means. Section 1168 of the 2006 Act states that electronic means includes e-mail or fax, and other means that are in an

electronic form *e.g.* documents sent on disk. A document is sent by electronic means if it is sent and received by electronic equipment or through wire, radio or optical means. The 2006 Act provides in Part 3 of Schedule 5 that information may be sent or supplied by a company if that person has agreed to the provision of information and such agreement has not been revoked.

As under the 1985 Act, a company can provide information to a person by the use of a website if that person has agreed to the use of such website.

The Companies Act 2006, the Disclosure and Transparency Rules, and the Listing Rules

The provisions relating to the use of electronic means for communications between a company and its shareholders need to be considered in conjunction with the provisions of the Disclosure and Transparency Rules ("DTRs"). The DTRs also came into force in January 2007 and govern the disclosure of information for financial instruments that have been admitted to trading on a regulated market, or to which an admission to trading on a regulated market has been made.

In the event that a company chooses to use electronic communication, it must comply with certain procedures set out in the DTRs. For example, the decision to provide information electronically must be taken in general meeting.

AIM Companies and the Use of Websites

The Alternative Investment Market ("AIM") is the secondary market in the United Kingdom. It has its own set of rules separate from the Listing Rules that apply to Main Market companies.

Post-admission, each AIM-listed company is required under AIM Rule 26 to maintain an up-to-date website to include the following information: (a) description of the company's business (and, if an investing company, its investment strategy); (b) information on directors (including biographical details); (c) a description of the responsibilities of the members of the board of directors and details of any sub-committees; (d) country of incorporation and main country of operation; (e) details of any other exchanges or trading platforms on which the company has applied to have or agreed to have its securities admitted or traded; (f) the number of shares traded on AIM, the percentage that are not in public hands, and the identity and holdings of significant shareholders with an update every six months; (g) copies of its current constitutional documents; (h) if not incorporated in the United Kingdom, a statement that the rights of shareholders may be different from those of a UK incorporated company; (i) details of any restrictions on share transfers; (j) the most recent annual report and any half yearly reports since the last annual reports; (k) any notifications made in the past 12 months; (m) any prospectus, admission, circular or similar shareholder publication published in the past 12 months; (n) details of the Nominated Adviser and other key advisers.

Main Market Companies and Use of Websites

Where the company has a website it must: (a) make available on its site all inside information announced via a Regulated Information Service ("RIS") by the close of the business day following the day of the RIS announcement; and (b) for a period of one year following publication, retain on its website all inside information that it is required to disclose via an RIS.

The Combined Code on Corporate Governance (the "Combined Code") issued by the Financial Reporting Commission also recommends that the results of general meetings, including the number of valid proxy votes and the number of votes for, against, and abstaining in respect of each resolution, is contained on a company's website. Additionally, where a Combined Code provision requires a company to "make information available," this information may be published on the company's website.

Finally, both the Prospectus Rules and the DTRs allow certain documents to be published on a company's website as an alternative to or as well as physical publication.

Advertising and Promotion of Investments

The FSA is the regulatory body of England and Wales in respect of the trading of securities. In order to advise, arrange or manage investments of securities, the person undertaking such regulated activity needs to be authorised by the FSA pursuant to the Financial Services and Markets Act 2000 (the "FSMA").

Social media is an attractive option for companies, investment advisers and brokers, and indeed third parties, to provide information on investments and investment strategies. However, care should be taken that compliance is made with the relevant financial promotion legislation.

Under section 21 of the FSMA, there is a general restriction that a person must not in the course of business, communicate an invitation or an inducement to engage in an investment activity such as the purchase of securities. However, this does not apply to financial promotions that

have been made by an authorised person or approved by an authorised person. A communication can be written or oral, and would therefore cover information on a social media website or sent by electronic communications.

Breach of section 21 of the FSMA is a criminal offence under section 25 of the FSMA and can lead to two years' imprisonment and/or a fine. Agreements entered into as a result of an unlawful financial promotion are potentially unenforceable under section 30 of the FSMA, and the person engaging in investment activity may be entitled to recover any money paid or property transferred under the agreement, and to be compensated for any loss as a result of having parted with the money or property. Furthermore, a communication of a misleading or inaccurate financial promotion could result in a claim for misrepresentation, criminal liability for misleading statements under insider dealing legislation, section 397 of the FSMA, and/or civil liability under the market-abuse regime.

The FSA's financial-promotion regime is intended to be media-neutral and to accommodate new methods of communication, such as via the Internet and other electronic media, as well as traditional methods of communication, such as newspapers, radio and television.

Individual advertisements on a website may constitute a financial promotion. However, the entire website may be a financial promotion if the sole function of the website is to advertise the services of a company for the purposes of inviting or inducing viewers to enter into investment activity.

The FSA is of the view that the person who causes the website to be created, *i.e.*, the person who is the owner of the website rather than the web designer or the Internet service provider hosting the website, is the "communicator" for the purposes of the FSMA. The FSA does not itself approve financial promotions. Instead, the financial promotion must be made either in reliance on an applicable exemption in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"), or it must be approved by an FSA authorised person. The FSA relies on the fact that senior management should take responsibility for the financial promotion pursuant to the Senior Management Arrangements, Systems and Controls ("SYSC") in the *FSA Handbook*.

A major difference between social media and traditional media is that the Internet has a far wider geographical scope than traditional methods of communication as it can be accessed, and information can be received, globally. This does raise the issue that it would be difficult to restrict access to persons in specific jurisdictions, and therefore a website could be subject to regulations of several jurisdictions.

The territorial scope of the financial-promotion regime under the FSMA is that any communication directed from the UK to another person, or a communication originating outside the United Kingdom where the communication is capable of having an effect in the United Kingdom, will fall under the FSMA.

There are a number of exemptions in the FPO in relation to geographical scope, the type of communication, the recipient, (*e.g.*, institutional investors, high net-worth individuals and overseas investors), the communicator (*e.g.*, journalists, overseas communicators and governmental authorities), communications relating to securities and listing matters (*e.g.*, promotions required or permitted by market rules, promotions of securities already admitted to certain markets) and company communications (*e.g.*, group companies and annual accounts and directors reports).

The financial promotion regime applies to both written and oral communications, where a communication is "made to" or "directed at" another person. A communication is "made to" another person if it is addressed verbally or in legible form to a particular person or persons, whereas a communication is "directed at" one or more persons if it is addressed to persons generally.

A distinction is made in many exemptions between real time and non-real time communications, and solicited and non-solicited real time communications. A "real time" communication is a communication made in the course of a personal visit, telephone call or other interactive dialogue. A "non-real time" communication is a communication that is not a real time communication. Financial promotions communicated via a website are deemed to be non-real time communications directed at one or more persons generally. As a rule, a greater number of exemptions apply to non-real time communications or solicited real time communications, as it is thought that recipients should be granted greater protection in circumstances where they are being asked to react immediately, or in "cold-calling" situations.

Financial promotions that are not subject to an exemption must be "clear, fair and not misleading" under the FSA's financial promotion rules. The rules for the financial promotion of securities can be found in chapter 4 of the *FSA's Conduct of Business Sourcebook* ("COBS') for savings and investments.

In 2007, the FSA undertook a review of 130 websites, of which only 75 percent were deemed to meet the FSA's standards.

Of the 25 percent of the websites that failed to reach the "clear, fair and not misleading standards" of the FSA, the firms had failed to present key information in a clear and logical manner (including risk warnings not being clearly presented, details of fees and exclusions being hidden in FAQ sections). In some instances general website maintenance was also lacking, resulting in out-of-date or incorrect information being provided to consumers.

The FSA is keen to ensure compliance with the standards it has set, and it has stated that it will take direct action against companies that are not in compliance. This could include requiring companies to amend the financial promotion or, in extreme cases, for the company to be fined or publicly named.

It is not only the content of the website itself that may be caught by the financial promotion regime, but also hyperlinks, banner advertisements and sponsored links.

Hyperlinks may or may not be a financial promotion in itself. Whether a hyperlink is a financial promotion will depend on the nature of the hypertext link and the context in which it is placed. However, taken in isolation, a hypertext link that is purely the name or logo of the destination will not be a financial promotion in its own right. More sophisticated links, such as banners or changeable text, may be financial promotions.

Material on a host website that contains the hypertext link may in itself be a financial promotion if it contains text that seeks to encourage or incite persons to activate the link with a view to engaging in investment activity.

Banner advertisements on a website are the Internet equivalent of an advertisement in a newspaper and are almost bound to be inducements. So whether they are inducements to engage in investment activity will depend upon their contents, as with any other form of advertising.

Sponsored links are text-based advertisements returned from keyword searches on a search engine or associated website. Depending on their content, a sponsored link and search engine results may also be a financial promotion, if they induce consumers to take out a regulated product or use a firm's services. Companies must, therefore, ensure all their communications, including sponsored links, are fair, clear and not misleading.

Social Media and the Market-Abuse Regime

Social media allows the dissemination of information to the public at large, and more and more investors are exploiting the use of social media, such as bulletin boards and blogs. There are dedicated forums on the Internet, such as share-forum.co.uk, Interactive Investors (iii.co.uk) and trade2win.co.uk, for investors to meet and discuss the trading of securities. These forums, together with the likes of Facebook and Twitter, mean that there is a real risk that price-sensitive or confidential information could be made public. The result of unauthorised disclosure of this information could be caught by the market-abuse regime under the FSMA and insider dealing rules under Part V of the Criminal Justice Act 1993 ("CJA").

The FSA continues to investigate and push for prosecutions in insider dealing. As recently as January 2010, three individuals have been arrested on charges of insider dealing.

Market Abuse

Market abuse is a civil offence under sections 118 and 118A of the FSMA. The FSA has published an on-line handbook, which in turn contains the Code of Market Conduct ("MAR"), which provides examples of matters that constitute market abuse.

The FSMA provides for seven different types of behaviour that constitute market abuse: (a) insider dealing; (b) disclosure of information; (c) misuse of information; (d) manipulating transactions; (e) manipulating devices; (f) dissemination; and (g) marketing distortion. Not all of the seven behaviours have a social media aspect, but those that do are considered below.

Insider Dealing

Insider dealing under s.118(2) of FSMA and MAR 1.3 is where an insider deals, or attempts to deal, in a qualifying investment or related investment on the basis of inside information relating to the qualifying investment.

This runs parallel to the criminal offences for insider dealing under Part V of the CJA. A person deals as an insider when: (a) he deals on a regulated market or through or as a professional intermediary in securities whose price would be significantly affected if the inside information were made public; (b) he encourages another person to deal on a regulated market or through or as a professional intermediary in such securities; or (c) he discloses the inside information, except in the proper performance of his employment, office or profession.

Information is held "as an insider" if the individual knows that it was acquired from an inside source and that it is inside information. Information is obtained from an inside source if the individual has obtained it: (a) because he is a director, shareholder or employee of an issuer (not necessarily the company or institution to which the information relates); (b) by virtue of his employment, office or profession; or (c) directly or indirectly, from a person noted in (a) and (b).

Information is "inside information" if: (a) it relates to particular securities or to a particular issuer or issuers and not to securities or issuers generally; and (b) it is specific or precise; and (c) it has not been made public; or (d) if it were made public it would be likely to have a significant effect on the price of any securities.

Insider dealing is punishable with imprisonment of up to seven years, or a fine, or both, under section 61 of the CJA.

In R v Neel and Matthew Uberoi (2009). Matthew Uberoi and his father, Neel Uberoi, were found guilty of 12 counts of insider dealing under section 52 of the CJA at Southwark Crown Court. Matthew Uberoi had been an intern at a corporate broking firm in 2006, working on a number of price sensitive deals. Uberoi passed inside information about deals in three companies to his father, who then purchased shares in those companies and made a profit of about £110,000 based on this inside information. Matthew and Neel Uberoi were subsequently sentenced to 12- and 24-months prison sentences, respectively, in December 2009. This information could, of course, have been obtained through a social media conduit.

Disclosure of Inside Information

Disclosure of inside information under s.118(3) of the FSMA is where an insider discloses inside information to another person other than in the course of his employment, profession or duties.

In November 2009, Alexei Krilov-Harrison, a stockbroker, was fined the sum of £24,000 for disclosing insider information to a number of clients in order to persuade them to buy shares in Provexis Plc. Krilov-Harrison had received inside information that Provexis, an AIM-traded company, had signed a major contract with an international food company. An announcement was scheduled to be released to the market in two days, and the company's share price was expected to increase as a result. Prior to the announcement, Krilov-Harrison disclosed the information by telephone to three clients who then proceeded to buy shares. Although the disclosure of the inside information was made by telephone, it could have been made through a bulletin board or a blog.

Manipulating Devices

Manipulating devices under s.118(6) of the FSMA and MAR 1.7 is when transactions or orders to trade employ fictitious or any other form of deception or contrivance.

An example of social media would be using a site such as Twitter or Facebook to voice an opinion about securities (or the issuer) while having previously taken positions on those securities subsequently from the impact of the opinions voiced on the price of that security, without having simultaneously disclosed that conflict of interest to the public in a proper and effective way.

Dissemination

Dissemination under s.118(7) of the FSMA and MAR 1.8 is the dissemination of information by any means that gives, or is likely to give, a false or misleading impression as to the value of securities by a person who knew or could reasonably be expected to know that the information was false or misleading.

An example of this would be if a person posts information on an Internet bulletin board or chat room that contains false or misleading statements about the takeover of a company, and the person knows that the information is false or misleading.

Misleading Statements and Market Manipulation

Making misleading statements and market manipulation are criminal offences under section 397 of the FSMA.

Misleading Statements

It is a criminal offence under s.397(1) of the FSMA for a person to: (a) make a statement, promise or forecast that he knows to be misleading, false or deceptive in a material particular, or dishonestly conceal any material facts; or (b) recklessly make (dishonestly or otherwise) a statement, promise or forecast that is misleading, false or deceptive in a material particular for the purpose of inducing, or being reckless as to whether it may induce, another person to enter, or offer to enter into, or refrain from entering or offering to enter into, a relevant agreement, or to exercise, or refrain from exercising any rights conferred by a relevant investment.

This would include, for example: a statement, promise or forecast that induces or is likely to induce a shareholder to sell or refrain from selling shares could constitute an offence if the person making the statement knew or was reckless as to whether it was misleading, false, or deceptive, or if it dishonestly concealed any material facts. It is easy to see how there could be a situation where an individual could post on a bulletin board or on Facebook or Twitter, and it would constitute a misleading statement.

The FSA commenced proceedings against four former directors of iSoft Group Plc – Patrick Cryne, Stephen Graham, Timothy Whiston and John Whelan – for conspiracy to make misleading statements to investors pursuant to s.397(1) of the FSMA, and the directors appeared before the City of Westminster Magistrates Court in January 2010. iSoft Group Plc had been under investigation since 2006 for accounting irregularities. iSoft had been engaged as a software supplier for the new £12.7 billion computer systems for the National Health Service. The company was forced to restate its profits for the financial years 2004 and 2005 because of a radical change in its accounting practices, as a consequence of the discovery that profits had been counted as soon as contracts had been awarded, as opposed to after the work had been completed and payment received. The restatement of profits meant that operating profit for 2005 was reduced from £72 million to zero, and revenues were revised from £262 million to £190 million. The revised figures led to a mass sell-off of shares by investors, leading to a 90 percent fall in the value of the company before its eventual sale to IBA Health Group, an Australian information technology company.

Market Manipulation

The criminal offence of market manipulation under s.397(3) of the FSMA is committed if: (a) any person does any act or engages in any course of conduct that creates a false or misleading impression as to the market in, or the price or value of, any investments; and (b) that person does the act or engages in that course of action (i) for the purpose of creating that false or misleading impression and (ii) for the purpose of thereby inducing that other person to deal or not to deal in those investments. As with a misleading statement, it is easy to see how a posting on a social networking site could lead to a charge of market manipulation if that statement would lead to a false or misleading impression as to the market.

The FSA won a recent case at the Financial Services and Markets Tribunal against Winterflood and two of its traders. In June 2008, the FSA found that Winterflood and its traders had played a pivotal role in an illegal share ramping scheme relating to Fundamental-E Investments Plc ("FEI"), an AIM-listed company. It was noted that the market maker had misused rollovers and delayed rollovers, thereby creating a distortion in the market for FEI shares, and misleading the market for approximately six months in 2004.

The FEI share trades executed by Winterflood had several features that should have alerted the market maker to the clear and substantial risks of market manipulation. However, instead of ensuring that the trades were genuine, Winterflood continued the highly profitable trading. Winterflood made about £900,000 from trading in FEI shares. The FSA decided to impose fines of £4 million on Winterflood, and £200,000 and £50,000 on the two traders as a consequence of their respective actions.

Archiving and Social Media

A number of regulations govern data breaches and archiving, which may well have an impact on social media.

Markets in Financial Instruments Directive (MiFID)

MiFID is a directive of the European Union designed for investment firms operating in the European Economic Area. MiFID contains a number of provisions designed to protect the integrity of financial transactions, including the transparency of transactions and types of information that must be captured when clients place trades. COBS specifically requires instant messaging conversations to be retained when trades are referenced. At the moment, Twitter is not used to transmit and execute trading orders. However, should it be so used in the future, such posts would also have to be retained.

FSA Handbook

The *FSA Handbook* contains a number of requirements that may have an impact on the use of social media. Pursuant to section 3.2.20 of the Senior Management Arrangements, Systems and Controls (SYSC) in the *FSA Handbook*, a firm must take reasonable care to make and retain accurate records of matters and dealing, including accounting records.

Under SYSC 9.1.1, a firm must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the FSA or any other relevant competent authority under MiFID to monitor the firm's compliance with the requirements under the

regulatory system, and in particular to ascertain that the firm has complied with all obligations to clients.

Under SYSC 9.1.2, a firm must retain all records kept by it in relation to its MiFID business for a period of at least five years.

In relation to the retention of records for non-MiFID business, a firm should have appropriate systems and controls in place with respect to the adequacy of, access to, and the security of its records, so that the firm may fulfil its regulatory and statutory obligations. As for retention periods, the general principle is that records should be retained for as long as is relevant for the purposes for which they are made, and that sensitive information is not leaked via social media.

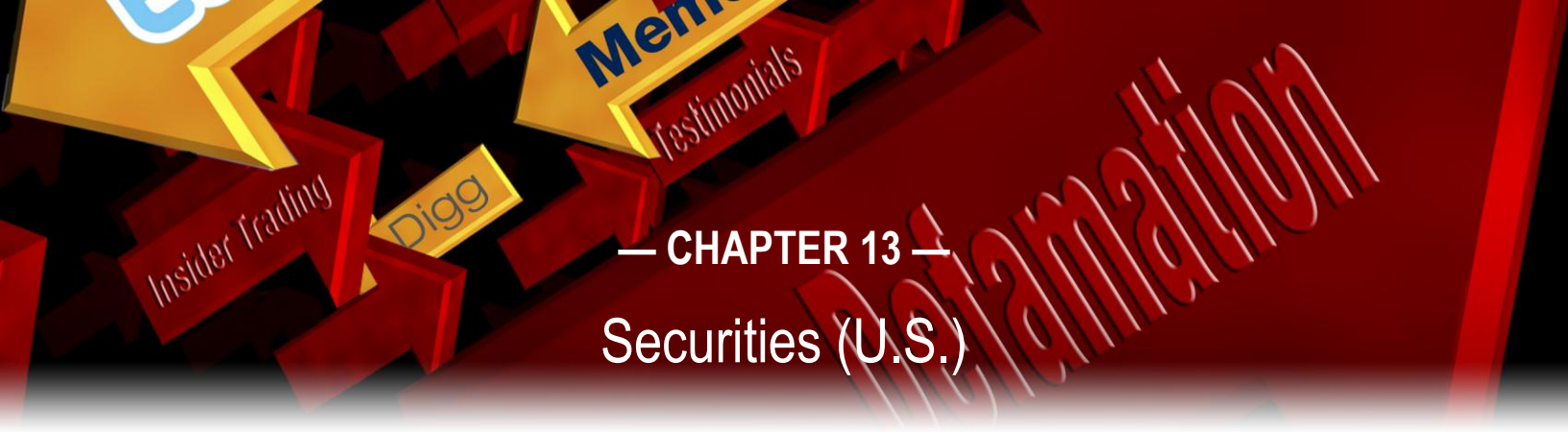
The FSA released Policy Statement 08/01 – Telephone Recording: recording of voice conversations and electronic communications in March 2008 that focuses on the use of electronic media and the need to retain information passing via electronic systems. Whilst social media (other than instant messaging) was not directly considered, it is advisable that similar consideration is given to social networking tools, and posts to social networking sites should be retained in the same way as instant messages would be.

Conclusion

When considering the appropriateness of the use of social media, care must be taken to ensure compliance with the relevant legislation.

Companies should ensure that when undertaking any form of financial promotion, the financial promotion complies with the “clear, fair and not misleading” standards of the FSA and is approved by a person authorised by the FSA, or that the financial promotion is subject to an exemption under the FPO.

Companies should ensure that they have adequate security procedures in place to prevent unauthorised access to confidential information, and that employees are aware of their obligations regarding the non-disclosure of price-sensitive information, and the appropriate use of electronic communications.



— CHAPTER 13 —

Securities (U.S.)

Chapter Authors

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

William M. Krogh, Associate – wkrogh@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 and 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.

While the majority of companies still distribute their earnings announcements and other investor disclosures through traditional paid public relations wire services, some large companies, such as Expedia, Inc. and Google Inc., are taking advantage of the SEC guidance on using company websites for disclosure under Regulation FD, and moving toward exclusively providing this information through their websites.

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 now recognizes more channels of distribution than in the past 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. The SEC has already made it clear that companies can use their websites for disclosure if their websites are a "recognized channel" for reaching investors. In time, other forms of social media may become recognized channels. In the short term, however, most companies would be well-advised to continue to rely on recognized forms of shareholder communication, while perhaps supplementing that approach with social media to more effectively reach actual or potential customers, investors, or shareholders. While social media presents an attractive channel of communication, care must be taken to ensure 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. The consequences of noncompliance become more severe if the recipients of the information selectively disclosed trade their shares ahead of a broad, non-exclusionary 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 on August 1, 2008, and subsequent compliance and disclosure interpretations issued on August 14, 2009, relating to the use of company websites for disclosures. These guidelines explain the general boundaries applicable to sharing information through social media outlets, as well as the potential for issuer liability for information the company or its employees post on blogs, networks, or discussion forums. While social media appears to be viable from a compliance perspective as a means to disseminate information to the public, issuers must establish internal policies that respond to the SEC guidelines.

Advertising and Promotion

Social media also offers an opportunity to provide information in connection with a transaction or to promote a particular investment or investment strategy. As such, it could be a very effective and attractive tool for investment advisers, investment companies and broker-dealers. If, however, 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. Although there are risks, numerous registered investment advisers ("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 ensure that they obtain the proper approval before using social media tools.

Broker-Dealers and Their Registered Representatives

For registered representatives ("RR") subject to Financial Industry Regulatory Authority ("FINRA") regulations, this means obtaining the approval of their broker-dealer compliance department before posting any business communication on the Internet. Static postings are considered advertisements, and FINRA has published guidelines for use of social media by registered representatives, in a regulatory notice issued January 25, 2010, clarified and expanded upon by a second notice issued August 22, 2011. The goal of these notices was to ensure that as the use of social media increases over time, investors are protected from false or misleading representations and that financial firms are able to effectively supervise their associated persons' participation in these forms of communication. The key issues addressed in FINRA's regulatory notices include the following:

- **Recordkeeping responsibilities**: Every firm that communicates through social media sites must retain records of any communications in order to comply with the Securities Exchange Act and NASD rules that require broker-dealers to retain electronic communications related to their business.

- **Suitability responsibilities**: If a firm recommends a security through a social media site, it is required to ensure that the recommendation is suitable for every investor to whom it is made under NASD Rule 2310. FINRA recommends that firms use those features of social media sites that limit the ability to access information to a select group of individuals in order to meet this requirement. Further, communications that recommend specific investment products may trigger, for example, the FINRA sustainability rule and other requirements under federal securities laws, which may create substantive liability for a firm or a registered representative.

- **Static versus interactive content**: Whether content posted by a firm or registered representative is "static" or "interactive" will determine which supervisory rules apply. Unscripted, real-time communications are considered interactive, although they may become static if reposted after they occur. A single social media website, page, or user account may contain both static and interactive content. For example, static postings may be made to a Facebook page, while the same Facebook account is used for interactive instant messaging. Each of these types of communication will be subject to different rules.

- **Approval or supervision of content posted on a social media site**: If the content to be posted on a social media site is considered to be static, it must be approved by a registered principal at the firm prior to posting. A material change to such a posting requires prior approval as well. If content to be posted is interactive and unscripted, pre-approval is not

required, but the firm must still monitor such posting to ensure that it does not violate applicable content requirements. Additionally, the firm is required to pre-approve the design of any relevant website created by an associated person, even if only interactive content will be posted there.

- **Supervision of social media sites**: A firm must adopt procedures and policies that are reasonably designed to ensure that communications through social media do not violate FINRA or Securities Exchange Act rules or laws. The supervisory system that will be optimal will be different for each firm, but some consistent themes are clear. The system should include a combination of prior review by a principal and retrospective review, with the precise mix depending on the nature of the communication. One investment firm has announced a program to allow its financial advisors to disseminate pre-approved updates through private messages using social media and to send invitations and introductions. The reaction of regulators to this approach deserves close attention. Above all, a firm must ensure through its policies and procedures that its associated persons who participate in social media for business purposes are appropriately supervised, have the necessary training and background for such activities, and do not present undue risks to investors.

- **Third-party posts**: When a third party posts content on a social media site established by a firm or its employees, FINRA generally does not treat such posts as the firm's communication with the public, and thus the responsibilities described above do not apply to those posts. However, the third-party content will be attributable to the firm if the firm has either involved itself in the preparation of the content or endorsed it explicitly or implicitly.

  In any event, third-party posts relating to the firm's business remain subject to recordkeeping requirements as communications received by the firm. Like third-party posts, third-party content linked from a firm's website will be attributable to the firm if the firm has been involved in its preparation or is deemed to have endorsed it.

  Additionally, a firm may not link to a third-party site if the firm knows or has reason to know that it contains false or misleading content. Having "reason to know" encompasses red flags that ought to prompt further investigation. More stringent requirements apply to a firm incorporating a third-party vendor's data feed directly into its website. The firm is under an affirmative duty to inform itself of the criteria used by the vendor to gather the data and must evaluate the proficiency of the vendor to supply accurate data. The firm also must periodically review the data for indications of unreliability.

- **Use of personal sites and devices by an associated person**: A firm's compliance responsibilities apply to all communications of its associated persons that concern the firm's business, regardless of whether those communications are made via the firm's website, social media account, or device or the associated person's personal website, social media account, or device. If a firm allows its associated persons to make business-related communications via their own personal means, it must supervise those means and follow record-retention requirements. Conversely, if the firm will not supervise and preserve records of a communication channel belonging to an associated person, it must prohibit the use of that communication channel for business-related communications. A firm must train its associated persons on the difference between business and non-business communications and on their duties with respect to the former.

Registered Investment Advisers

Statements of RIAs and their representatives amounting to advertisements, which include most postings about the firm made to publicly accessible forums, are subject to similar requirements under the Investment Advisers Act of 1940 and SEC rules. Those sources also contain record-retention requirements that apply more broadly, not only to advertisements.

Illustrating its interest in the area of social media, the SEC issued a broad document request to RIAs in February 2011 concerning employees' use of the technologies. The SEC published a summary of its findings in a January 2012 Risk Alert, which contains some useful guidance.

RIAs are generally responsible for self-supervision by chief compliance officers. In light of that, RIAs have perhaps somewhat greater flexibility than those subject to FINRA regulations when using social media. Nevertheless, care should be taken to avoid publishing securities recommendations or any testimonials, both of which are explicitly prohibited by the SEC and state regulatory authorities. Additionally, 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.

- **Testimonials**: Certain types of social media, expressly or implicitly, violate the prohibition on testimonials contained in Rule 206(4)-1(a)(1) under the Investment Advisers Act. A testimonial is a statement relating to a client's experience with, or endorsement of, an RIA or its representative.

  The SEC's January 2012 Risk Alert suggests that tools in the nature of the "like" button on Facebook may constitute testimonials, that RIAs should consider measures to disable their use, and that more robust monitoring might be required if disabling the tools is not possible, so that offending content can be removed swiftly. If a mere "like" on Facebook may constitute a testimonial, then a professional recommendation on LinkedIn is of even greater concern.

  It should be understood that a "like" or a recommendation posted with reference to an RIA or its representative may constitute a testimonial regardless of whether it was solicited or volunteered. And it may constitute a testimonial regardless of whether its author is a client or only a friend or family member of the RIA's representative.

- **False or misleading statements**: Recommendations are also likely to be viewed as false or misleading if motivated by an undisclosed interest of the recommender. Recommendations, being recommendations, also have the inherently misleading characteristic of excluding criticism. Thus, recommendations posted on social media might violate Rule 206(4)-1(a)(5), which bars any advertisement that is false or misleading in any way.

  Twitter and Facebook present additional dangers of false or misleading statements. RIA representatives may send messages in haste, thereby increasing the risk of inaccuracy. A tweet is limited to 140 characters, which leads to the use of abbreviations, raising the risk of inadvertently misleading language. Necessary qualifications and disclosures may be left out.

  Profiles on LinkedIn, Facebook, and other social media platforms should be scrutinized to ensure that they are not false or misleading and should be consistent with the RIA's advisory contract, as well as with its website and other advertisements. All references to performance may be subject to the SEC's guidance in the Clover Capital no-action letter, which 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 must take care not to violate 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.

- **Supervision of social media sites**: RIAs should ensure that their compliance manuals incorporate policies and procedures regarding the use of social media by their employees. RIAs have four general options: (1) allow employees to post information about the advisory firm but require pre-approval by the firm's compliance department (a supervisory nightmare); (2) allow posting, but only of pre-approved content created by the firm and provided to employees for that purpose; (3) allow posting only to forums that are not publicly accessible; or (4) categorically prohibit the posting of any information about the firm, other than the mere fact of the poster's employment, whether in a public or private forum.

  The SEC's January 2012 Risk Alert emphasizes that the policies a firm adopts should be risk-based, meaning tailored to the particular risk factors that a firm faces and selected after evaluating the effectiveness of existing policies. The Alert states that retrospective review of posted content, as opposed to prior approval, may not be adequate under all circumstances. Also, although the appropriate level of monitoring may be achievable only with the help of outside vendors, the firm remains responsible for the adequacy of those measures.

  The Alert also warns of a duty to monitor any changes in the operation of a social media site that might compromise client privacy. The SEC seems to be envisioning a scenario in which an RIA's or representative's privacy settings initially conceal information regarding its contacts, but then a design change exposes the information unless new settings are elected. If the protection of client information cannot be ensured, the Alert goes on to say, then the use of the site may not be appropriate.

  Training is a critical component of any RIA's compliance regime. 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 rules and firm policies and procedures. An advisory firm should

also require all employees to affirm that they are in compliance with the firm's rules regarding advertising and electronic communications. The firm's chief compliance officer should also periodically inspect popular social media sites for violations of either Rule 206(4)-1 or the firm's own policies and procedures.

- **Security**: The Risk Alert warns of the potential for social media to serve as an entrée to hackers. It advises maintaining appropriate walls to separate sensitive information from social media sites.

- **Recordkeeping responsibilities**: The Investment Adviser's Act imposes similar recordkeeping requirements to those applicable broker-dealers. The SEC's January 2012 Risk Alert emphasizes that the content of a communication, rather than the medium, determines whether it is subject to recordkeeping requirements. If a particular social media channel is not compatible with recordkeeping requirements, then it should not be used for communications that are subject to those requirements. Training, monitoring, and other policies should be designed to achieve that end.

  One recent enforcement action brought by the SEC[318] underscores the point. An alleged fraudster operating an RIA was accused of, among other violations, communicating with prospective clients via a web-based email account, LinkedIn, and Trade Key, each of which automatically deleted messages after six months, while he did nothing to preserve the communications.

Even the SEC is now using Twitter, underscoring its attention to social media. 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 is capable of finding compliance violations in social media.

Insider Trading

Social media's "stock in trade" is information, and some of the information that might be conveyed via social media is material non-public information. The transmission of such information, if it breaches a duty to the company or person from which it was obtained, may itself be a violation of the securities laws, and trading on such information typically means liability for insider trading. All such conduct is regulated primarily through the antifraud provisions of the securities laws, most often Section 10(b) of the Securities Exchange Act 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. In addition, the SEC's new organizational structure, announced in 2009 and put into place last year, includes specialized subject-matter units within the Division of Enforcement, including a Market Abuse Unit focused on investigations into large-scale market abuses and complex manipulation schemes by institutional traders, market professionals, and others. The Market Abuse Unit relies heavily on computers, cross-checking trading data with personal information about individual traders, such as where they went to school or used to work, to find like trading patterns among possible associates. Suffice it to say, social media will be a critical source of information for this specialized team.

These innovations, together with recent pressure on U.S. regulators in the wake of high-profile enforcement failures, are likely to result in increased enforcement in the area of insider trading. This is particularly true because insider trading cases are comparatively easy for regulators to identify and investigate. Meanwhile, recent years 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 violators. 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.

Social media is of particular importance to insider trading issues because of the volume of information traffic, the cross-border nature of that traffic, and the opportunity for regulators to locate the source of the information. Social media postings—like everything on the Internet—never really disappear.

Unregistered Offerings

Section 5(c) of the Securities Act of 1933 makes it unlawful to offer a security unless a registration statement has been filed with the SEC or an exemption from registration applies. Although this registration requirement is common knowledge among seasoned participants in the securities markets, it is not so well known among the general public. Social media enables novel and spontaneous forms of collective action that may amount to an offering of securities without those involved realizing that the

securities laws are implicated at all. In June 2011, the SEC entered a cease-and-desist order[319] against two individuals who had attempted to "crowdsource" a purchase of the Pabst Brewing Company. Crowdsourcing, as the SEC order put it, "is the use of social media and the Internet to organize a large group of individuals to achieve a common goal, in this instance, to raise capital." The private owners of the Pabst Brewing Company were seeking to sell the company. The two defendants, whose backgrounds were in advertising, created a website, complemented by a Facebook page and Twitter account, called BuyaBeerCompany.com. The pair solicited pledges toward a stated goal of raising $300 million. If that goal was met, the pledges were to be collected. At that point, each investor was to receive a "crowdsourced certificate of ownership" and, eventually, an allotment of beer as well.

The website succeeded in garnering more than $200 million in pledges over the course of four months. Only then did the defendants consult with an attorney. It does not appear that they considered the possible application of the securities laws before that time.

Even if the offering had been registered or exempt, it appears to have also run afoul of the prohibition on general solicitations of investors, although the SEC did not raise that issue.

The matter was resolved with a cease-and-desist order after the website was taken down. Had the defendants actually collected money from investors, however, the legal consequences might have been much more severe for them. The case illustrates the potential and the risk of social media to enable inexperienced securities market participants to reach large numbers of investors.

Both the SEC and Congress are currently considering measures to loosen registration requirements when entrepreneurs raise small amounts of capital from large numbers of investors. These initiatives were inspired at least in part by the BuyaBeerCompany.com matter. Regardless of the eventual outcome of reform, those looking to raise capital should remember that an offering of securities made via social media remains governed by the same rules as one made via traditional media. To undertake an offering of securities requires thorough familiarity with applicable registration requirements, as well as rules governing what sort of investors may participate and how they may be solicited.

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 use the power of social media to unlawfully influence share price. Companies should monitor social media outlets to ensure that information is being properly and lawfully dispersed.

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–just one variety of market manipulation–and social media is the perfect place for false rumors to grow and eventually impact stock prices. Although companies will not be able to prevent all such manipulation, reporting the activity to regulators (and to website hosts) in the first instance is just one approach that should be discussed with counsel.

Current Legal and Regulatory Framework in the Securities Sector

Four recent actions brought by the SEC and FINRA offer cautionary tales. Although only one actually involved the use of social media, each offers lessons of particular applicability to the compliance risks associated with social media.

Violation of FINRA Rules

In a recent disciplinary action,[320] FINRA found that a registered representative created two websites, without the approval of her employer firm, that misrepresented her career accomplishments and the firm. Also without approval, the registered representative made a number of unduly positive posts to her personal Twitter feed concerning a security of which she and members of her family possessed substantial holdings. Although there is no indication that regulators have taken any disciplinary action against the employer firm, the incident exemplifies the sort of employee misuse of personal social media accounts and websites for which financial firms may be held responsible if their compliance policies and procedures are found lacking. As the August 2011 FINRA guidance makes clear,

broker-dealers must affirmatively prohibit their associated persons from using personal websites and social media accounts to make business-related communications, or else they must supervise those accounts and websites. Adequate training regarding the difference between business and non-business communications, and the rules that apply to the former, is also necessary to avoid imputation of responsibility to a financial firm for the actions of an unscrupulous associated person.

Violation of Regulation FD

In *SEC v. Black*,[321] 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 that second quarter earnings would be in line with first quarter earnings, the defendant sent email from his home to eight analysts who covered the company, advising that second quarter earnings would likely fall short of expectations by half. 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 email, it could have 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 a recurrence. 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 disclosed the information on a Form 8-K. Had the unauthorized disclosure occurred via social media, the existence of policies specific to the use of social media would likely have carried additional weight with the SEC.

More recently, the SEC filed a civil injunctive action against Presstek, Inc., and its former President and CEO, Edward J. Marino, for violations of Regulation FD and Section 13(a) of the Securities Exchange Act.[322] The SEC charged that Marino took a call from Michael Barone, the managing partner of Sidus, an investment adviser whose funds held substantial positions in Presstek. The call between the two is documented in Barone's notes and text messages that he sent to colleagues at Sidus during and after the call.

According to the SEC's complaint and Barone's notes, Marino revealed during the call that "[s]ummer [was] not as vibrant as [they] expected in North America and Europe," and that while "Europe [had] gotten better since [the summer]…overall a mixed picture [for Presstek's performance that quarter]." During the course of these disclosures from Marino, Barone sent a text to a Sidus colleague, saying, "sounds like a disaster." That colleague inquired as to whether he should buy Presstek puts, and Barone confirmed. After the call, Sidus began selling, and Barone sent a text to the Sidus trader "sell all prst," which he did. Coincident with those sales, Presstek's stock dropped 19 percent. Presstek accelerated disclosure of its poor quarterly earnings numbers, issuing the report the next day, with the result that the stock dropped another 20 percent.

Presstek settled with the SEC without admitting or denying liability, agreeing to pay a $400,000 civil penalty. The Commission acknowledged substantial remedial measures taken by the company, including the replacement of its management team. Marino continues to fight the charges.

The case is interesting on a number of levels, particularly since there are probably many who would wonder whether the statements attributed to Marino rise to the level of material non-public information, which is likely why the matter is charged solely as a Regulation FD violation, with no insider trading charges. But there is no question that the comments cited are just the sort of generalities that might show up in a tweet or a Facebook newsfeed.

False Rumor

In *SEC v. Berliner*,[323] 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. Over a 30-minute period, the price of ADS stock plummeted 17 percent, causing the New York Stock Exchange to temporarily halt trading in the 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 on an issuer's stock price.

Insider Trading

Although the misappropriated disclosures in *SEC v. Gangavarapu*[324] were made during telephone calls between siblings, the facts disclosed are of exactly the sort you would 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. The defendant's sister told him when her husband was in closed-door meetings, that he was working long hours, and that he had traveled overseas for work. 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. After the public announcement that CSC would acquire Covansys, the price of Covansys' stock rose 24 percent, resulting in trading profits for the defendant totaling more than $360,000.

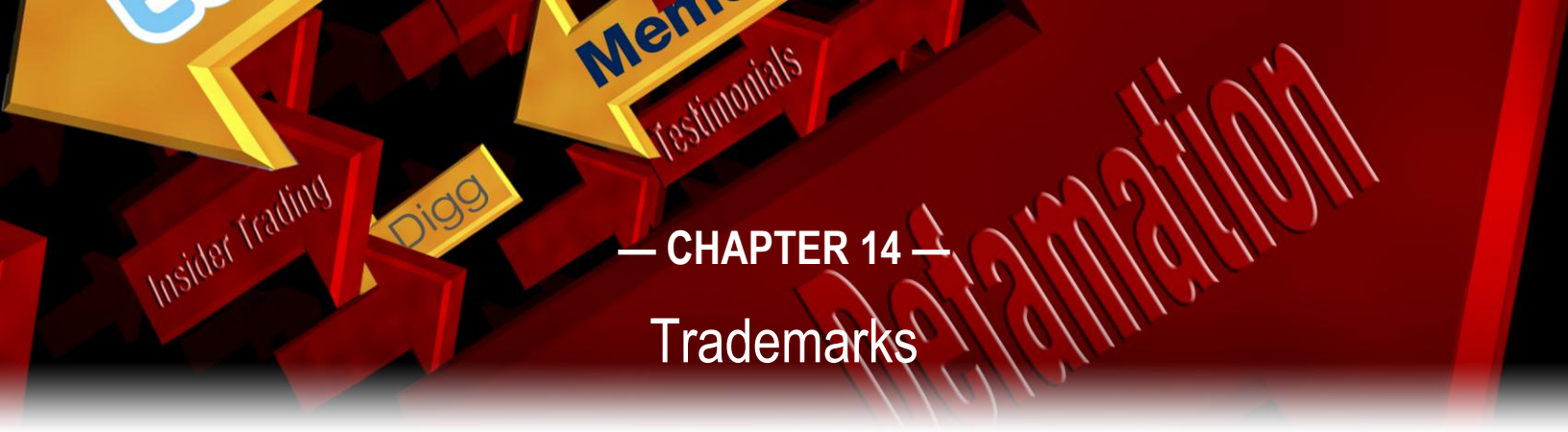
Bottom Line—What You Need To Do

Before you decide to adopt social media 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 regulatory requirements. For material disclosures, that means compliance with Regulation FD. For advertising of transactions or services, that means ensuring that you obtain the proper approval before using social media and that you are not in violation of any regulations, such as the Investment Advisers 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 Internet and social media presence to ensure that the discussion is appropriate, that 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, conduct routine searches for the use of your company's name and corporate logo or other image, so as to ensure 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. If a violation should occur, 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 14 —

Trademarks

Chapter Authors[325]

United States:

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

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

Germany:

Dr. Alexander R. Klett, Partner – aklett@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 perpetual. 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 unauthorised use of their trademarks, service marks and trade names are emerging through these same channels.

First, we will examine trade mark 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 discuss 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, personalised sub-domain names, virtual products, and avatars, which all create confusion as to 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") has experienced meteoric growth since its launch in July 2006, with almost 75 million visitors in January 2010 alone.[326] 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 which is 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.[327] 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 unauthorised account. After the complaint was filed, however, the parties resolved the dispute and the account has since been transferred to the company.

A more complex situation arose for Vodafone, whose UK Twitter account was hijacked internally (with a tweet we cannot reproduce here for reasons of taste) by a (presumably now ex) employee[328].

If the Vodafone case proves that companies must have robust internal policies on consumer-facing social network activity, third-party "Twitterjacking" is less easily dealt with. 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.[329]

And while Twitter provides such a policy, it is unclear how well-developed a plan it has for dealing with trademark infringement 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 to be 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:

Facebook

Facebook has more than 400 million active users, allowing its members to connect with others, upload photos, and share Internet links and videos. A recent Compete.com study ranked Facebook as the most-used social network by worldwide monthly active users.[330]

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.[331] 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.[332]

Facebook also reserves its right to remove or reclaim a username upon complaint by a trademark owner.[333]

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 registered trademark. The question of jurisdiction is also unclear. If a Community Trade Mark (CTM) is registered in Europe, to what extent will a claim citing infringement by a U.S. user hold water? How will Facebook handle claims by multiple parties claiming rights in the same mark? Only time will tell.[334]

In its own effort to combat trademark infringement and name-squatting, Facebook, in conjunction with its new policy of allowing users to create personalised 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 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 each profile and for each of the pages that a user administers.
- In an effort to prevent a user from monopolising a commercially desirable term, generic words may not be registered as a username.

Though these efforts can help provide some comfort to trademark owners, it is unfeasible to protect any and all variations in the 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?

Another limitation is that common law and other unregistered rights to names under domestic laws (whether in the United States, the UK or continental Europe) are not part of this policy. In other words: If a trademark is not registered, a brand owner cannot automatically prohibit its use as a Facebook URL.

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 an action for trademark infringement or unfair competition are options to protect a valuable trademark.

What Constitutes Infringement?

In the United States, 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…"[335] Similar "use in commerce" requirements exist for claims of unfair competition[336] and dilution.[337] 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 commercialisation.

Under English law, as generally under trademark laws in the member states of the European Union that are harmonised under the EU Trademark Directive,[338] trademark infringement occurs where a registered trademark is used without the owner's consent, and:

- The sign used by the infringer is identical to the registered trademark and is used in relation to identical goods or services
- The sign is identical to the registered trademark and is used in relation to similar goods and services
- The sign is similar to the registered trademark and is used in relation to identical or similar goods or services, and there is a likelihood of confusion by the public, or
- The sign is identical or similar to the registered trademark, the trademark has a reputation domestically, and the use of the sign takes unfair advantage of, or is detrimental to the distinctive character of, the trademark[339]

Under European Community trademark law, the CTM Regulation[340] provides the proprietor of a CTM with the right to prevent third parties from using:

- A sign that is identical to the CTM in relation to identical goods or services, or
- A sign identical or similar to the CTM in relation to identical or similar goods or services if there exists a likelihood of confusion by the public.

The European Court of Justice (ECJ) has held[341] that mere adoption of a company name does not constitute trademark infringement. The test used by the ECJ was that the use of the sign must affect the mark's essential function of guaranteeing source. It is likely that the adoption by a third party of a name in a social media context will pass this test, though each case will depend on its facts. If use of the company name in a social media context is made in a way that clearly indicates that the use does not originate from the company itself (*e.g.*, a username such as "BMWcritic), infringement will likely not be found.

The English courts have also addressed the question of jurisdiction.[342] In the *1-800 Flowers* case, it was held that for trademark law purposes, website-use did not constitute use everywhere in the world merely because the site is globally accessible. Key factors to determining infringement

were held to be the intention of the website operator and what local users understand upon accessing the site. Applying this test to Facebook, Bebo or MySpace could result in different decisions depending on geographical coverage and demographic reach. Decisions in other European countries, such as Germany,[343] have used the same approach and asked whether the website-use is directed at the respective domestic customers or audience.

Unfair Competition/Passing Off

In English law, companies can use the tort of passing off to protect their brands. A company looking to protect its name, mark or get-up must establish goodwill, misrepresentation and damage to successfully argue passing off.

While an action for trademark infringement can only be brought in relation to a registered trademark, the cause of action in passing off is wider and protects all elements by which a claimant's business can be identified. That said, passing off is narrower in scope and harder to prove than the law of "unfair competition" in the United States. While the tort of passing off has not yet been tested in a social media context, there is no reason for it not to apply, albeit that it might be difficult to prove damage in this context. If this is the case, a claimant can instead rely on an argument based around erosion of goodwill, which has previously been successful in the English courts, if the claimant's brand exclusivity has been reduced, blurred or diminished.[344]

While unfair competition law is not harmonised within the European Union to the same degree as trademark law, other countries offer similar (albeit not identical) remedies to passing off. In Germany, for example, the imitation of goods or services of a company leading to an avoidable confusion among consumers as to commercial origin, or unjustly exploiting or impairing the goodwill connected to the imitated goods or services, constitutes unfair competition.[345] The one case decided by German Courts in this context did not concern an individual use within a social media context, but rather an alleged imitation of the look and feel of Facebook by the German site StudiVZ.[346]

Impersonation

Social media websites such as Twitter and Facebook have 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.[347]

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

> The profile information on a parody 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.[348]

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.[349] 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 unauthorised and offensive messages under his name.[350] Specifically, he claimed that the unauthorised 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 settled in June 2009.

Cases like this beg the question as to how well trademark owners can rely on social media websites to shut down imposters, even in light of such matters being brought to their direct attention. In the UK, the advent of personalised URLs may allow trademark owners to rely on English case law, which has held that use of a domain name can infringe a registered trade mark. In Germany, the courts are at least as generous, and have not only viewed the use of a domain as infringing trademark rights, but also as infringing rights to personal and company names.[351]

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 who 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 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.[352]

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. Ironically, many famous celebrities delegate the use of their Twitter account to their publicist or manager.

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 socialise, connect and create using voice and text chat, also allows users to create virtual products for sale online, using online currency to complete the transaction that is purchased with real world currency. Habbo is another example, only with a broader reach and targeted to a teen and pre-teen audience.

Trademark Infringement

Too often the virtual products offered for sale on virtual worlds bear the trademarks of third parties without permission to do so. By way of example, in the United States, Taser International, Inc. filed a trademark infringement claim against Second Life over the sale of unauthorised virtual versions of its electronic stun guns.[353] The lawsuit was later dropped, but the liability of Linden Lab, creator of Second Life, was debated in the media.[354] 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 unauthorised trademark should be held liable, not the party who merely provided the platform. In Europe, the E-Commerce Directive makes no such distinction. Thus, virtual world operators might seek to rely on the argument that they are mere conduits, expeditiously removing infringing content when put on notice. Equally, brands that are struggling to find recourse in the United States may find solace in Europe.

A further question is whether such use of another's trademark, in fact, amounts to trademark infringement. After all, these unauthorised products are not actually offered for sale in the real world, only online. However, several trademark owners have actively promoted the use of their products on Second Life, including International Business Machines Corp. and Xerox Inc.[355] 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.

In the European Union, the ECJ found that use of a trademark protected for toys on a toy replica of a car will constitute trademark infringement only if that use affects or is liable to affect the functions of the trademark, or if, without due cause, use of that sign takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trademark.[356] In the *Adam Opel* case, which followed a preliminary ruling from a German court, the German courts ultimately found no such harm to the trademark, and therefore no infringement.[357]

As intellectual property lawyers 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 unauthorised 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 trade mark rights or serving as a barrier to potential licensing opportunities and avenues.[358]

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 unauthorised copies of its virtual adult-themed animated bed, using Eros' "SexGen" mark.[359] 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.[360] Eros had owned a pending application with the U.S. Patent and Trademark Office for the mark "SexGen" (which has since matured to registration)[361], and a second plaintiff, DE Designs, owned a federal registration for the mark "DE Designs."[362] 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 unauthorised copying and distribution of the plaintiffs' products
- Represent to the court under penalty of perjury that any remaining unauthorised 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 that operate entirely within a virtual world nevertheless receive recognition of their marks, at least in the United States (though maybe not in Europe, depending on the facts at issue), 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.[363] This can certainly be seen as a step ahead for trademark rights within virtual media. Why do companies bother with these lawsuits? Because the virtual economy is growing at a massive rate (witness Zynga, for example), and younger generations are learning their first hand experiences online.

In an EU law analysis, it is difficult to see how a sale of virtual goods will constitute a sale of goods for legislative purposes. As discussed, harmonised trademark law in the European Union turns on whether the goods and services related to the alleged infringer are identical or similar to the trademark owner's goods and services (unless, under some domestic laws, use in commerce is made of a famous brand). To what extent will the courts decide that virtual Louis Vuitton wallpaper is similar to the real thing? This issue has not been decided (yet) in the English courts.

In the UK, brand owners might opt to rely on passing off, which, as discussed, does not turn on similarity but instead requires goodwill, misrepresentation and damage to be established. In other EU countries, similar remedies under unfair competition law may be available.

So, how do brand owners protect themselves? One option concerns registration for different classifications, such as for online interactive games (Class 41). EU member states adopt different approaches in this regard. Under UK law, an applicant must honestly intend to make goods and services available in the classes for which it registers a mark. This differs from the Office of Harmonization for the Internal Market ("OHIM") practice, which permits broad registrations, and regulates undue scope through the provisions on revocation for non-use. This seems like a simple change to make in return for extending the protection of your brand. Some EU member states adopt a similar approach. In Germany, for example, applications need to be made in good faith in the sense that bad faith applications can be challenged. However, in practice the application is regarded as neutral so long as there is no actual indication of bad faith on the part of the applicant (which would have to be demonstrated by the party challenging the application). EU member states (along with the CTM regime) also employ a revocation procedure for non-use once five consecutive years of non-use after registration have passed. Furthermore, the hurdles set by the ECJ will still apply even if trademark protection exists for relevant services in Class 41.

Perhaps to prove it is a good copyright citizen, Second Life, like Twitter and Facebook, has a policy in place to help avoid infringement and impersonation.[364] Your account name cannot be the name of another individual to the extent that it could cause deception or confusion; a name that violates any trademark right, copyright, or other proprietary right; a name that may mislead other users to believe you to be an employee of Linden Lab; or a name

that Linden Lab deems in its discretion to be vulgar or otherwise offensive.[365]

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…[366]

Linden Lab is generally known to remove any content from its site that incorporates another's trademark without the trademark owner's authorisation, or features the unauthorised use of celebrity material, as evidenced by the case wherein the Trump organisation 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 organisation 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 unauthorised 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.[367] 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. As in other areas, this is the beginning of the development of "virtual laws,"" where virtual worlds seek to operate under their own distinct and unique legal framework, often based on real legal principles.

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, in the United States at least, 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.[368] 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."[369] The case settled.

As these cases evidence, trademark owners and providers of virtual world platforms remain ever vigilant of the growing concern regarding the unauthorised 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 a 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 unauthorised use of such marks and works of authorship.

— CHAPTER 15 —

The U.S. Patent Minefield

Managing Risk Resulting from Assertions by Non-Practicing Entities (NPEs)[370]

Chapter Author

Marc S. Kaufman, Partner – mkaufman@reedsmith.com

Introduction

Risk resulting from patent infringement allegations has always been high in the United States. The emergence of the Non-Practicing Entity (NPE) model has served to increase this risk. NPEs are sometimes referred to as "patent trolls" because of their attempt to assess a fee on the activities of alleged infringers (referred to as "targets" herein). The typical business model of an NPE is to assert patents and generate revenue from licensing fees or damage awards assessed by courts. NPEs, as the name suggests, do not compete in the marketplace that they claim is covered by their patents. Therefore, traditional mechanisms of leverage used against competitor patent assertion, such as counterclaims for patent infringement, a partnering deal, a cross license for patents or other intellectual property, and the like, are not effective to assert leverage against NPEs. This, combined with the aggressiveness of NPEs because of their revenue model, has led to a significant increase in risk because of patent infringement in the United States. Companies operating in the areas of digital media, advertising, and financial services are particularly vulnerable as a result of the large amount of relevant patents that were originally owned by start-ups that did not succeed. Often, these patents end up in the hands of NPEs.

To be clear, the typical NPE revenue model is perfectly legal. NPEs range from venture capitalists purchasing patents on the open market for a return on investment, to innovators who have developed significant technology only to see it misappropriated by large companies without remuneration. However, the frustration and uncertainty caused by this business model has led to various changes in the common law and statutes.[371] The NPE business model, though, will likely remain legal and perfectly viable in the foreseeable future. Therefore, a good strategy for managing the risk presented by NPEs is necessary when doing business in the United States. This article will avoid the discussion of visceral and emotional reactions to the NPE model in favor of articulating constructive approaches to managing risk and uncertainty.

It is important to understand the typical NPE value proposition. Most NPEs will offer a license that, while expensive, will likely be less than the costs of taking the NPE to trial and less than the cost of evaluating the patent in some cases. The proposition presented by the typical NPE is, "for X dollars, we (the NPE) will provide a guaranteed result (license to the patents) as opposed to paying a multiple of X dollars to your lawyers and experts with no guarantee." Sometimes this value proposition is not unreasonable. However, there are ways to apply leverage and present risk to the NPE that will, at the very least, reduce "X" significantly. Of course, there are situations where a license is the best approach and others where a license is not appropriate.

The NPE revenue model leverages the uncertainty and inefficiencies that are inherent in patent defenses. Patents are often complex legal and technical documents, and the patent laws in the United States are far from simple. In order to truly understand the scope of a patent, it is often necessary to review and interpret thousands of pages of technical documents, and the history of the proceeding before the U.S. Patent and Trademark Office that resulted in the patent. On the other hand, NPEs often utilize contingent fee attorneys and thus have little out-of-pocket expense. This imbalance is the foundation of the NPE revenue model.

However, the target of the NPE assertion can present risk to the NPE. A successful defense against an NPE assertion requires demonstrating to the NPE that:

- The NPE is at risk of having the patent assets declared invalid or otherwise unenforceable
- The assertion will take a great deal of time and will be expensive to the NPE
- The target has the resolve to go to trial if necessary
- The industry players will cooperate to reduce costs for the targets

By demonstrating that it is sophisticated and has resolve, the target of the NPE assertion becomes a less desirable opponent and thus eliminates some of the leverage of the NPE. The five key components to a successful resolution of an NPE assertion are:

- Risk assessment
- Aggressive license negotiation tactics
- Aggressive litigation (when necessary)
- Creative legal fee models
- Industry collaboration

Risk Assessment

It is critical to understand the risk presented by the NPE assertion before beginning negotiation in earnest. NPE assertions range along a spectrum from "nuisance," in which the NPE does not have a strong legal position and is looking merely for a modest payment, to high risk, in which the NPE has a strong legal position against a significant product or service being offered by the target. It is helpful to place the assertion on this spectrum. While the target and the NPE will likely disagree on the relative legal strength of the NPE assertion, each party, in most cases, will understand the position of the assertion on this spectrum, plus/minus a "point of view" (POV) value. While some NPEs are completely unreasonable, most are quite sophisticated these days and understand the strengths and weaknesses of their legal position. Accordingly, if the target has evaluated its own legal position, the parties are, for the most part, on the same page (even if the parties do not admit to this).

It may be difficult to admit, however, that some NPE assertions have solid legal and factual bases and are best treated as such. Therefore, it important to asses risk. The best approach is a step-by-step approach. While there is no single recipe for evaluating risk, the following will provide some guidelines. Of course, some of the activities can be conducted in parallel and the order prescribed below is not optimum in all cases.

First, a title search on the asserted patents should be conducted. It is not unheard of for a party to try to assert patents that it does not have a right to assert. Also, in some instances the target has the benefit of a license to the asserted patents granted to a supplier or the like. A title search is not difficult to conduct. At this time, it is also worthwhile to investigate any potential indemnity, through supplier contracts or the like, and to comply with any notice provisions thereof.

Next, it is important to gather as much information as possible on the NPE, its targets, its business model, and settlement terms. For example, has the NPE filed suit before? If so, what was the outcome and did the outcome affect the value of the asserted patents? What tactics has the NPE used for licensing/settlement? Who is counsel for the NPE and what is counsel's reputation? The answers to these questions will help ascertain what you are up against and will help you begin to place the assertion along the spectrum noted above. In many cases, the outcome of your research on the NPE may indicate that there is an opportunity for settlement at a very low dollar amount. While settlement may seem "distasteful," it may be the best business choice if the matter can be disposed of for a relatively small amount.

If the steps above do not lead to a resolution, it is important to determine the likelihood that the alleged conduct actually infringes the asserted patents. This is accomplished by having counsel review the patent(s), the record of prosecution of the patent before the Patent Office, and

technical details of the accused activity. Counsel can then make a determination of the strength of the infringement allegation. If the non-infringement position is extremely strong, it can often be used to negotiate a favorable settlement, or even to convince the NPE to drop the assertion.

If the infringement position is subject to doubt because of possible claim construction issues, a validity analysis of the asserted patent(s) should be conducted. Such an analysis includes a thorough search of the relevant prior art and an analysis thereof by patent counsel to determine if the patents are not novel and non-obvious, and thus are likely to be invalidated by a court. A strong position of invalidity will, of course, provide settlement leverage. Finally, a high-level damages analysis should be conducted to ascertain the amount of revenue and profit as a result of the alleged infringing activity.

License Negotiation

Once the requisite-level risk analysis has been accomplished, the target can begin to negotiate a license/settlement with the NPE. As noted above, license negotiation can occur in tandem with risk analysis and thus, depending on the situation, the "requisite level" of risk analysis varies based on specific circumstances. At the outset, the target should press the NPE for details, such as how the asserted patent claims map to accused activities and the amount of any initial settlement demand. Also, based on the risk analysis, the target should soon present information to the NPE demonstrating that the NPE has risk as a result of potential invalidity and/or non-infringement. Also, if the damages analysis shows that the NPE is not likely to achieve a large reward, such evidence possibly should be presented at this time.

Regardless of the circumstances, the target should demonstrate the ability and resolve to make the assertion difficult for the NPE. Counsel with a strong patent litigation reputation should be retained and mitigating evidence from the risk analysis should be presented. Notwithstanding the above, the target should define "success" in the matter and be open to a settlement that is within the range of this definition.

Litigation

If license negotiations are not productive, embarking upon some level of litigation may be necessary. Of course, the target can let the natural course of litigation unfold by waiting for the NPE to file suit in a venue of the NPE's choice. Alternatively, it may be desirable to be proactive and put pressure on the NPE. One tactic is to file for a review of the patent through one of the administrative review proceedings in the U.S. Patent Office. Another way to reduce leverage of the NPE is to file a Declaratory Judgment action in a venue of the target's choice prior to any suit being filed by the NPE. Whether litigation is filed by the NPE or the target, the target might want to push for early claim construction and/or quick Summary Judgment. Of course, any use of the tactics above depend on the forum and specific facts of each case. Finally, nontraditional counterclaims, such as false advertising, unfair competition and other antitrust claims, should be considered. While such claims are not always available, they are becoming more acceptable by some courts.

Legal Fee Models

As noted above, the typical NPE model leverages the traditional legal fee models, typically hourly rates or fixed fees per matter, in which there is a high incremental cost for each litigation matter. However, to the extent that a legal fee model can be negotiated that reduces the incremental costs per litigation matter, the NPE has reduced leverage and the target is empowered. One example is a legal fee model in which a fixed monthly or yearly fee is paid to a law firm in exchange for a specified package of legal services throughout the year. The package of legal services and the fee can vary, of course. The concept is that the target has purchased a sort of "insurance policy" at a predictable rate and removed the incremental cost, and related budgeting issues, of individual matters that arise throughout the year.

Industry Collaboration

Since NPEs often assert against multiple players in a single industry, it is axiomatic that the various players in an industry can benefit from collaboration. Since the players are often competitors, this can require a careful balancing of how much information can be shared. However, the benefits far outweigh the balancing efforts. Collaboration can be at one or more levels. For example, collaboration may be limited to permissible sharing of information about the NPE's tactics and demands, sharing information about prior art, and sharing legal analysis (when approved by counsel).

Collaboration may be in the form of a joint defense agreement among targets or may be elevated to a broader collaboration of all industry players through a trade association or other entity. More creative opportunities for collaboration include the organized challenge of patents that are perceived to be an industry threat, or even a

purchase of patents to "take them off the street." Further collaboration can include accepted shared indemnities within an industry. Of course, antitrust counsel should be consulted before embarking on any collaborative activity among competitors.

Bottom Line—What You Need to Do

While the threat of NPEs cannot be eliminated—at least not in the short term—many tactics can be used to reduce uncertainty and thus reduce NPE leverage. Reduced NPE leverage means reduced risk for the target. Potential targets of an NPE should investigate all of the tactics outlined above, and any others presented by the specific facts, in order to reduce the uncertainty presented by the various NPE patent assertion models.

— Biographies of Authors and Editors —

Sara A. Begley, Partner – Philadelphia · +1 215 851 8214 · sbegley@reedsmith.com

In addition to counseling employers on the scope of employment issues, Sara is a trial attorney with background in litigating cases involving race, age, disability, and gender discrimination, sexual harassment and retaliation. She has also tried other employment-related and breach-of-contract cases in the federal and state courts and before administrative and arbitration tribunals. Her most recent jury trials involved claims of race, age and disability discrimination which resulted in defense verdicts for our clients. A significant portion of her practice involves trade secret and restrictive covenant litigation which includes litigating preliminary and permanent injunctions in state and federal court. She also drafts and negotiates executive agreements, arbitration agreements, restrictive covenant and confidentiality agreements, severance packages, other employment-related agreements and contracts, employee handbooks, Affirmative Action Plans, and employer policies and procedures.

Paul Bond, Partner – 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.

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 counselling to a multitude of advertising agencies and brand owners on all matters of trademark law.

Eugene K. Connors, Partner – Pittsburgh +1 412 288 3375 econnors@reedsmith.com

Gene guides small and not-so-small local, national and international companies on how to best balance employer-employee needs to eliminate employment concerns while maximizing management options. Examples include acquiring, consolidating, relocating, automating, "right sizing," or closing businesses; retaining or regaining union-free status; and negotiating hundreds of agreements with affordable, flexible working conditions critical to global success. Beyond strategic planning and problem avoidance, Gene represents employers before federal and state courts; federal, state and local administrative agencies; arbitrators; and mediators.

Colleen T. Davies, Partner – San Francisco · +1 415 659 4769 · cdavies@reedsmith.com

Colleen is a member of the Life Sciences Health Industry Group, practicing in the area of product liability litigation. Colleen first joined Reed Smith in January 2003 when the firm combined with Crosby, Heafey, Roach & May. Her legal career has focused her civil litigation practice in the area of complex product liability defense. Her litigation and trial experience include national counsel responsibility for cases at the state and federal trial court levels, including multi-district litigation and class actions. Colleen's client base primarily consists of major pharmaceutical, medical device, software, hardware, electronic and consumer product manufacturers. While her experience extends into various product manufacturing arenas, her specialty areas remain in pharmaceutical, medical device and consumer product liability defense. She also counsels product manufacturers on all phases of product development. Here, her work addresses manufacturing and marketing issues such as product warnings, design development, document retention policies, claims management, media relations and crisis management. She also has experience establishing in-house systems for compliance with Consumer Product Safety Commission reporting obligations.

Stephen Edwards, Partner – London · +44 (0)20 3116 2910 · sedwards@reedsmith.com

Stephen is an expert in copyright and broadcasting law, handling both rights-related and other commercial transactions and regulatory work for clients ranging from start-up ventures to some of the media industries' household names. In the past year, for instance, he has worked on matters for the BBC, Channel Four, MTV, RTÉ and the European Broadcasting Union. He also has experience in dealing with EU legislation in the copyright and regulatory fields, most recently the EU Audiovisual Media Services Directive. In addition to television, radio and digital media work, Stephen's experience also covers music rights, sports agreements and all forms of print and online publishing.

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.

Peter Hardy, Partner – London · +44 (0)20 3116 2958 · phardy@reedsmith.com

Peter is a partner in the European Litigation Group and is an insurance recovery and reinsurance expert. He specialises in insurance recovery and reinsurance litigation and is recognised as a leading insurance recovery and reinsurance litigator in London. His practice covers a diverse range of insurance recovery and reinsurance disputes but reflects his particular experience in commercial crime and financial institutions' fidelity policies and other key commercial liability covers such as E&O, D&O and Pensions Trustee Liability. He is experienced in matters concerning the crossover between life insurance and pensions and the liability insurance market and has advised extensively on policy wordings and policy programme structures and reinsurance arrangements as well as in connection with issues arising upon the insolvency of an insurance company.

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.

Marc S. Kaufman, Partner – Washington, D.C. · +1 202 414 9249 · mkaufman@reedsmith.com

Marc specializes in assisting his clients in managing and monetizing their intellectual property assets. He has developed structured procedures for defining and executing intellectual property strategies that are aligned with overall business objectives, for a wide variety of business entities. From procuring and enforcing rights both in the United States and abroad to structuring and negotiating intellectual property transactions, Marc uses his skills and experience to help his clients achieve all of their objectives, Marc possesses a unique ability to understand the needs of his clients and to deliver relevant, timely and practical intellectual property related business and legal advice. Specifically in the area of patents, Marc has developed and managed patent portfolios that have been widely licensed by major corporations. Often times, he guides his clients in the sale of patents, that are no longer relevant to core objectives.

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.

Dr. Alexander R. Klett, Partner – Munich · +49 (0)89 20304 145 · aklett@reedsmith.com

Alexander is a partner in the German Intellectual Property (IP) group, responsible for all "soft" IP matters, and a commercial lawyer with international experience in a wide range of IP law matters, both contentious and non-contentious. Alexander advises regularly on prosecution, portfolio management, licensing, and infringement matters, particularly in the areas of trademarks, designs, copyrights and unfair competition. He advises on IP issues involving corporate transactions, and has advised on several high-profile disputes before the German and European Community authorities and courts involving trademark and copyright law matters. His clients include high-tech companies, financial investors, clients from such industries as clothing, watches and household goods, as well as film studios, entertainment companies and publishers.

Emma Lenthall, Partner – London · +44 (0)20 3116 3432 · elenthall@reedsmith.com

Emma is a commercial litigator and she jointly heads Reed Smith's Intellectual Property, Media, Advertising and Technology disputes group. She has acted on high profile defamation matters involving well known celebrities, newspapers and other individuals and organisations. She has also worked on copyright, trade mark and passing off matters for clients with famous brands. She regularly advises on clearance issues in relation to advertising and promotions and in the areas of privacy and confidence. Emma assists in the protection of a very well known intellectual property portfolio and has also worked on international arbitrations and professional negligence matters. She is a full member of Equity.

Paul Llewellyn, Partner – London · +44 (0)20 3116 3469 · pllewellyn@reedsmith.com

Paul is a member of the Life Sciences Health Industry Group, practising in the area of product liability litigation. Paul is Head of UK Product Liability and practises exclusively in product liability defence work. In the early years of his career his practice involved large scale actions and disease cases on behalf of trade union members. Over the last 20 years he has worked for major corporates and their insurers and leads a team of seven lawyers involved in product liability litigation and regulation, specialising in particular in medical device and pharmaceutical work. Paul has unique experience in negotiating innovative bespoke ADR agreements, having been responsible for negotiating the Capital Hip Claims Protocol on behalf of 3M and the Trilucent Breast Implant Protocol on behalf of the Inamed Corporation of Santa Barbara. These procedures have helped to resolve thousands of cases, either by the successful rejection of claims or their negotiated settlement, economically and efficiently without recourse to formal legal proceedings.

Mark S. Melodia, Partner – Princeton · +1 609 520 6015 · mmelodia@reedsmith.com

Mark leads the Global Data Security, Privacy & Management practice as a partner within the Global Regulatory Enforcement Group. He has recognized experience in litigating putative class actions and other "bet-the-company" suits. He works on behalf of clients in a variety of industries, including, but not limited to, financial services, media, and retail. He has succeeded in getting complaints dismissed, class certifications denied and/or favorable settlements negotiated on behalf of these clients. He has organized, led and participated in successful mass defense efforts involving claims of data breach, securities fraud, predatory lending, multi-state attorneys general and other government investigations, as well as allegations of antitrust conspiracy and deceptive sales practices.

Kathyleen A. O'Brien, Partner – Century City · +1 310 734 5268 · kobrien@reedsmith.com

Kathyleen is a partner in Reed Smith's Advertising, Technology and MediaGroup. She represents consumer products and media and entertainment companies in federal and state litigation and enforcement actions, including false advertising and antitrust litigation, consumer class actions involving unfair and deceptive advertising and trade practice claims and trademark and copyright infringement actions. She also regularly counsels clients on advertising, marketing, branding, privacy and data collection and use issues, oversees an active trademark and copyright prosecution practice, and conducts compliance programs, internet and employee training in these areas.

Cynthia O'Donoghue, Partner – London · +44 (0)20 3116 3494 · codonoghue@reedsmith.com

Cynthia is a partner in the European Corporate Group and a core member of the firm's multi-disciplinary Outsourcing Group. Cynthia specialises in large, complex IT and business process outsourcing transactions and advises on all aspects of sourcing and procurement-related transactions for both customers and service providers in the health care/life sciences, financial services, technology and telecommunications sectors. Cynthia also regularly advises on data privacy and cloud computing issues.

Gregor J. Pryor, Partner – London · +44 (0)20 3116 3536 · gpryor@reedsmith.com

Gregor is a partner in the Advertising, Technology and Media team. He has broad experience of advising clients concerning the acquisition, production, licensing and distribution of content on digital media networks and platforms. He regularly advises content owners such as film and television production companies, record labels, music publishers and advertisers regarding the protection and exploitation of their intellectual property rights. He also advises companies that are involved in the distribution and sale of digital content, such as social networks, online retailers, aggregators, network operators, platform owners and search engines, regarding their arrangements with content owners and consumers. Gregor also advises clients concerning data protection and privacy matters, particularly in relation to online operations and targeted advertising.

Laurence G. Rees, Partner – London · +44 (0)20 3116 3545 · lrees@reedsmith.com

Laurence has specialised in employment law work since 1980 and advises clients drawn from a wide range of industrial and commercial sectors, on all aspects of employment law. Laurence has extensive experience of service agreements and other contracts of employment, and of consultancy arrangements, employment aspects of transactions, and executive compensation. He is regularly instructed on redundancy and workforce restructuring exercises, and the employment aspects of outsourcing. Laurence frequently advises on terminations of employment, often at boardroom level and the negotiation and documentation of settlement terms. Laurence also has significant expertise in the commercial aspects of UK immigration law.

Stephan Rippert, Partner – Munich · +49 (0)89 20304 160 · srippert@reedsmith.com

Stephan is a partner in the European Corporate Group and also responsible for the German Advertising, Technology & Media (ATM) practice. He is a commercial lawyer with international experience in a wide range of sophisticated and complex transactions. Stephan regularly advises on all contractual, commercial and regulatory ATM transactions including content distribution, digital and wireless media, licensing, syndication and production agreements, IT-Outsourcing and BPO, advertising and sponsoring, media concentration rules, software, e-commerce, intellectual property, data protection, privacy issues, unfair competition, and litigation. His practice also encompasses joint ventures, mergers & acquisitions and strategic alliances. Stephan has advised on several major transactions in Germany with respect to the acquisition of the German broadband systems and digital platform operations. His clients include international broadcasters, U.S. film studios, new media companies, software and technology companies, food and steel companies, and financial investors. Stephan also advises clients in the life sciences sectors medical devices, biotechnology and pharmaceuticals on a wide range of transactional and regulatory matters.

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

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and 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.

Nicolas C. Sauvage, Partner – Paris · +33 (0)1 76 70 40 00 · nsauvage@reedsmith.com

Nicolas Sauvage is recognized as one of the experts of social law in France. He joined the Paris office of Reed Smith in April 2010 as the leading partner of the Labour and Employment Team. Nicolas assists employers with the various aspects of human resources management. He handles both individual and collective working relationship matters, and social security disputes. He treats highly sensitive cases applying technical knowledge and expertise in labour and employment law and has an invaluable local and market knowledge to the particularities of various business sectors. He advises and guides companies through restructuring, mergers and acquisitions, establishment of operations outsourcing, collective redundancies, but also in recruitment and organization procedures, the deployment of expatriation policy, social aspects of immigration law, operations, investment and disinvestment by foreign companies in France. As regards Social Security, Nicolas assists companies in the social security audits or during investigations relating to industrial accidents and occupational disease and specialized courts. He regularly speaks at conferences on labour and employment law topics in France and abroad, particularly on discrimination topics.

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).

Michael J. Young, Partner – London · +44 (0)20 31163655 · myoung@reedsmith.com

Michael specialises in advising clients in respect of a broad range of corporate finance and company/commercial transactions, including cross-border and domestic takeovers, mergers and acquisitions, joint ventures and equity issues by public and private companies. Michael has extensive experience in acting for companies on their admission to the markets of the London Stock Exchange and subsequent fundraisings. Michael has particular experience of acting for clients in the media and technology and financial services sectors.

Louise Berg, Associate – London · +44 (0)20 3116 2831 · lberg@reedsmith.com

Louise focuses on intellectual property and media law and has advised on disputes involving trade mark issues, copyright law, design right, defamation, privacy and breach of confidence. She also advises on non-contentious intellectual property matters, assisting clients with clearance work and issues relating to trade mark registrations and licences. She has experience in digital distribution and e-commerce issues and her work in this area includes advice on user generated content, Internet piracy, domain name disputes and liability under IT services contracts. Louise also advises on general commercial disputes and was engaged on a large multiparty case involving insurance, film finance, allegations of fraud, professional negligence and breach of contract.

James Boulton, Associate – London · +44 (0)20 3116 2844 · jboulton@reedsmith.com

James joined Reed Smith in 2007 having joined from a boutique corporate practice in Birmingham. He is an associate in the European and Middle Eastern Corporate Group, advising clients on company/commercial and transactional matters.

Carl De Cicco, Associate – London · +44 (0)20 3116 2892 · cdecicco@reedsmith.com

Carl trained at Reed Smith and joined the Employment Group upon qualification in September 2005. He undertakes a broad spectrum of employment work and has advised clients in relation to matters involving unfair dismissal, discrimination on grounds of race, sex, disability and age, whistleblowing and breach of contract. Carl has also been involved in the employment aspects of a large number of corporate transactions, both business sales (involving the application of TUPE) and share sales. Carl also advises clients with matters involving contracts of employment, redundancy situations and the enforcement of garden leave provisions and restrictive covenants.

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.

William M. Krogh, Associate – Philadelpia · +1 215 851 8273 · wkrogh@reedsmith.com

William joined Reed Smith in spring 2011 and is a member of the firm's Global Regulatory Enforcement Group.

Kevin M. Madagan, Associate – Washington, D.C. · +1 202 414 9236 · kmadagan@reedsmith.com

Kevin is a member of the Life Sciences Health Industry Group, practicing in the area of health care regulatory law. His practice encompasses a wide range of regulatory, litigation, corporate and contractual matters. Kevin works with numerous health care entities, including, pharmaceutical companies, medical device manufacturers, pharmacies, and health care providers—hospitals, skilled nursing facilities, rehabilitation facilities. In addition, Kevin has experience with FDA and USDA regulated food entities. Kevin assists clients with marketing issues, product development, product launches, clinical trials, contract negotiation, importation issues, seizures, regulatory due diligence, regulatory filings, internal fraud and abuse investigations, corporate transactions, regulatory appeals (*e.g.*, PRRB, DAB), and government inspections and investigations.

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.

Huw Morris, Associate – London · +44 (0)20 3116 2816 · hmorris@reedsmith.com

Huw is an Associate in the Advertising, Technology and Media Group and a founding member of the Reed Smith Advertising Compliance Team (ReACTS). He has extensive experience in Intellectual Property, digital, contractual and regulatory matters, advising some of Reed Smith's major clients in the advertising, media, gaming and FMCG sectors. He joined Reed Smith from the Institute of Practitioners in Advertising, where he advised an impressive client list of the major UK advertising agencies on a wide variety of legal issues relevant to the advertising industry. Since joining Reed Smith, he has undertaken a number of successful secondments to high-profile clients, providing a wide range of advertising/media compliance and general commercial advice. He is a regular speaker at events hosted by the Advertising, Technology and Media Group, and recently spoke on the subject of social media marketing at a conference in Belgrade, Serbia, hosted by one of the world's largest independent advertising agency networks.

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.

Katharina A. Weimer, Associate – Munich · +49 (0)89 20304 160 · kweimer@reedsmith.com

Katharina is a member of the European Corporate Group and focuses in the area of Advertising, Technology & Media (ATM). She is a commercial lawyer with a strong focus on all media and entertainment related matters. Among her clients are international broadcasters as well as new and old media enterprises. She also has substantial experience in copyright-related contentious and non-contentious matters, international and national data protection matters and all aspects of doing business on the Internet. Katharina's main focus is supplemented by continuous advice in life sciences and clinical trial projects, involvement in various international transactions and litigation and extensive experience in agreements for the virtual world.

— 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 *New York Times*, Oct. 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 The authors wish to acknowledge the contributions of Marina Palomba to the content of this chapter.

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

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

16 *See*, "Web Ad Spend Outstrips TV for First Time," *The Times*, Sept. 30, 2009.

17 *Id*.

18 *Id*.

19 David Goetzl, "Kellogg Increases 2010 Ad Spend, Triples Social Media," *MediaDailyNews*, Feb. 18, 2010 (http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=122709).

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

21 *Id*.

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

23 http://www.facebook.com/promotions_guidelines.php

24 *Id.*

25 Mike Kornacki, "Social Media Contests – Participation is Not Always Easy to Come By," SocialMediaToday.com, Jan. 21, 2010 (http://www.socialmediatoday.com/SMC/168344).

26 *Id.*

27 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.

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

29 *Id*.

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

31 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.

32 16 CFR Part 255.

33 16 CFR § 255.l(d).

34 http://fastlane.gmblogs.com

35 http://thelab.gmblogs.com

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

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

38 *Id*.

39 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.

40 *Doctor's Associates Inc. v. QIP Holders LLC*, 82 U.S.P.Q.2d (BNA) 1603 (D. Conn. April 18, 2007).
41 Joseph Lewczak, "Quiznos/Subway Settlement Poses Threat to Future UGC Promos," *PROMO* Magazine, March 23, 2010.
42 Bundesgerichtshofentscheidung dated Nov. 12, 2009 (AZ I ZR 166/07, marions.kuchbuch.de).
43 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.
44 *See,* Cass R. Sunstein, "On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done," (Farrar, Straus, and Giroux 2009).
45 The Impact of the Class Action Fairness Act of 2005 on the Federal Courts.
46 15 U.S.C. § 45.
47 15 U.S.C. § 1125(a).
48 15 U.S.C. § 45.
49 Available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm
50 *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).
51 *Int'l Harvester Co*., 104 FTC 949 1058 (1984).
52 *Sandoz Pharmaceuticals v. Richardson-Vicks*, 902 F.2d 222, 228 (3d Cir. 1990).
53 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).
54 *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).
55 *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.").
56 *U.S. Healthcare*, 898 F.2d at 921 (3d Cir. 1990) (quoting 2 J. McCarthy, Trademarks and Unfair Competition § 27:713 (2d Ed. 1984)).
57 *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).
58 *See, e.g.*, *Ramson v. Layne*, 668 F.Supp. 1162 (N.D. Ill. 1987).
59 FTC Guides, at 5, n.11.
60 FTC Guides, § 255.0.
61 FTC Guides, at 8.
62 15 U.S.C. § 45.
63 FTC Guides, § 255.1(d).
64 FTC Guides, at 38-39.
65 FTC Guides, § 255.1(d).
66 FTC Guides, § 255.1(d).
67 FTC Guides, at 42.
68 *Id*.
69 FTC Guides, at 15.
70 *Id*.
71 FTC Guides, at 39.
72 FTC Guides, at 40, 42.
73 *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).
74 540 F.Supp.2d 288 (D.N.H. 2008).
75 *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).
76 The CAP Code can be found on CAP's website at http://www.cap.org.uk.
77 Restatement, Second, Torts § 558.
78 *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).
79 *E.g., Stratton Oakmont v. Prodigy*, 1995 WL 323710, at *3 (N.Y. Sup. Ct., May 24, 1995) (Unreported).
80 *E.g., Cubby v. Compuserve*, 776 F.Supp. 135 (S.D.N.Y. 1991).

81 47 U.S.C. § 230 ("CDA").
82 47 U.S.C. § 230(c)(1).
83 47 U.S.C. § 230(f)(3).
84 474 F.Supp. 2d 843 (W.D. Tex. 2007).
85 In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), for example, the Ninth Circuit dismissed a claim for negligence where the claim was more clearly tied to a failure to take down offensive speech.
86 474 F.Supp.2d at 849.
87 *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).
88 *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).
89 *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").
90 540 F.Supp.2d at 295-96 (emphasis in original).
91 *See 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").
92 2009 WL 3240365, No. 102578/09 (N.Y. Sup. Sept. 15, 2009).
93 2009 WL 3240325, at *1.
94 2009 WL 3240365, at *1 (*citing Blumenthal v. Drudge*, 992 F.Supp. 44, 52 (D.D.C. 1998)).
95 478 F.3d 413 (1st Cir. 2007).
96 *Id*. at 421.
97 521 F.3d 1157 (9th Cir. 2008) (*en banc*).
98 *See Nemet v. Chevrolet Ltd. v. Consumeraffairs.com*, 591 F.3d 250, 256-257 (4th Cir. 2009) (distinguishing *Roommates.com*, the Fourth Circuit holds, among other things, that defendant is not encouraging illegal conduct).
99 *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).
100 47 U.S.C. § 230(e)(2).
101 *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").
102 488 F.3d 1102 (9th Cir.), *cert. denied*, 128 S.Ct. 709 (2007).
103 *Id*. at 1118-19.
104 540 F.Supp.2d 299-304. *Accord*, *Atlantic Recording Corporation v. Project Playlist*, 603 F.Supp.2d 690 (S.D.N.Y. 2009).
105 O'Grady v. Superior Court (Apple Computer, Inc.), 39 Cal.App.4th 1423 (Sixth Dist. 2006).
106 2010 WL 1609274, A-0964-09 (N.J. Super. A.D., April 22, 2010).
107 2010 WL 1609274, at *11.
108 *Id.*
109 175 F.3d 848 (10th Cir. 1999) (affirming dismissal of claims directed to credit ratings based on First Amendment).
110 2003 WL 21464568, No. CIV-02-1457-M (W.D. Ok., May 27, 2003).
111 *Abu Dhabi Commercial Bank v. Morgan Stanley & Co., et al*, slip op. 08 Civ. 7508 (SAS) at 34 (S.D.N.Y. Sept. 2, 2009), *quoting In re IBM Corp. Sec. Litigation*, 163 F.3d 102, 109 (2d Cir. 1998).
112 *Id.* at 34-35 n.126 (quoting 175 F.3d at 856).
113 *Cats and Dogs Hospital v. Yelp, Inc*. CV10-1340VBF (C.D. Cal. 2010); *Levitt v. Yelp, Inc*., CGC-10-497777 (Superior Court, San Francisco, 2010).
114 Clifford, "Video Prank at Domino's Taints Brand," http://www.nytimes.com/2009/04/16/business/media/16dominos.html (April 15, 2009).
115 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
116 Art. 15 (1) of the Directive: Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
117 *Bundesgerichtshof* [German Federal Court of Justice], GRUR 2004, p. 860 – Internet auction I.
118 *Bundesgerichtshof* [German Federal Court of Justice], GRUR 2007, p. 708 – Internet auction II.

119 See, for example, *Bundesgerichtshof* [German Federal Court of Justice], GRUR 1999, p. 418.

120 17 U.S.C. § 102 (a).

121 S. 1 (1) UK Copyright Designs and Patents Act.

122 § 2 (2) German Copyright Act.

123 Such as in § 51 German Copyright Act.

124 The author wishes to acknowledge the contributions of Rachel A. Rubin to the content of this chapter.

125 YouTube Advertising Information Page, http://www.youtube.com/advertise.

126 YouTube Advertising Information Page, http://www.youtube.com/advertise.

127 Most ISPs, including YouTube, do advise users not to use copyrighted words, and counsel them on how to avoid infringement. YouTube posts an intellectual property protection policy on its site and notifies users that they should not use copyrighted material without permission in its terms and conditions. YouTube Terms of Service, http://www.youtube.com/t/terms. YouTube also has a Copyright Tips page that defines copyright protection and tells users how to avoid infringing someone else's copyright:

> Posting copyright-infringing content can lead to the termination of your account, and possibly monetary damages if a copyright owner decides to take legal action (this is serious—you can get sued!). Below are some guidelines to help you determine whether your video is eligible or whether it infringes someone else's copyright. YouTube Terms of Service, http://www.youtube.com/t/terms. YouTube Copyright Tips, http://www.youtube.com/t/howto_copyright.

Finally, YouTube's Terms of Service requires users to agree that they will not post any submissions that are subject to third party proprietary rights.

128 Full text of the DMCA: http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:

129 YouTube Copyright Infringement Notification, http://www.youtube.com/t/copyright_notice.

130 YouTube Content Verification Program, http://www.youtube.com/t/copyright_program.

131 YouTube Content Management, http://www.youtube.com/t/contentid.

132 Scribd.com Homepage, http://www.scribd.com/.

133 YouTube on Brand Channels, http://www.youtube.com/watch?v=kJv9F8W1p-w; http://www.youtube.com/watch?v=894IYciqYmc&feature=channel.

134 *Id.*

135 YouTube Insight, http://www.youtube.com/watch?v=Xo6HBKTyIzQ; YouTube Blog, Broadcasting Ourselves ;), *More statistics coming to a video near you* (July 22, 2009), http://youtube-global.blogspot.com/2009/07/more-statistics-coming-to-video-near.html.

136 Facebook Advertising, http://www.facebook.com/advertising/?src=pf.

137 Facebook Statistics, http://www.facebook.com/press/info.php?statistics.

138 Facebook Statistics, http://www.facebook.com/press/info.php?statistics.

139 Facebook's copyright policy for advertisers reads:

> Adverts cannot include any content that infringes upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary right.
> The advertiser must have intellectual property rights to the creative and be permitted to display such creative as advertising on the Facebook Site.

Facebook Advertising Guidelines, http://www.facebook.com/terms.php?ref=pf#/ad_guidelines.php.

140 Facebook Copyright Policy, How to Report Claims of Copyright Infringement, http://www.facebook.com/terms.php?ref=pf#/legal/copyright.php?howto_report

141 Facebook Copyright Policy, How to appeal claims of copyright infringement, http://www.facebook.com/terms.php?ref=pf#/legal/copyright.php?howto_appeal=1.

142 *See, e.g.,* Sally M. Abel, *Trademarks and Rights of Publicity in the Converged World*, 978 PLI/pat 57, Sept. 2009.

143 *Id.*

144 *Id.*

145 AppData.com – Facebook Application Metrics, Leaderboards for Sunday, January 24, 2010, (Jan. 24, 2010), http://www.appdata.com/.

146 Caroline McCarthy, *Why Facebook Left Scrabulous Alone*, The Social – CNET News (Aug. 1, 2008), http://news.cnet.com/8301-13577_3-10003821-36.html?tag=mncol.

147 http://blog.nielsenwire/nielsenwire/online_mobile/twitters-tweet-smell-of-success/

148 On April 13, 2010, Twitter announced that it will begin to host advertisements on its site. These will not be traditional ads, but rather "promoted tweets" targeted at certain people based on their searches on the site, based on the Google advertising model. *Twitter to have paid tweets show up in searches*, AP Newswire (Apr. 13, 2010), http://www.google.com/hostednews/ap/article/ALeqM5h51oZKi0PpOIcpnnsbgdzpseGf1AD9F27S1O0.

149 Twitter, Terms of Service, http://twitter.com/tos.

150 Twitter, Terms of Service, http://twitter.com/tos.

151 In March 2009, Courtney Love, Kurt Cobain's widow and lead singer of the band Hole, was sued in Los Angeles by a fashion designer who had done work for her, who claims that Love posted a series of mean-spirited defamatory and libelous Tweets

about her. Andrew Johnson, *Love's online spat sparks first Twitter libel suit*, The Independent (Mar. 29, 2009), *available at* http://www.independent.co.uk/news/media/online/loves-online-spat-sparks-first-twitter-libel-suit-1656621.html.

152 *Iran Protesters Using Tech to Skirt Curbs*, CBS News.com (June 15, 2009), http://www.cbsnews.com/stories/2009/06/15/earlyshow/leisure/gamesgadgetsgizmos/main5088668.shtml.

153 Jessica Lum, *News Wire Allegedly Steals Iconic Haiti Photo, Then Sues Photographer*, (Apr. 27, 1010), http://www.petapixel.com/2010/04/27/news-wire-allegedly-steals-iconic-haiti-photo-then-sues-photographer/; Dan Kennedy, *Haitian Copyright Case Turns on Twitter's TOS*, (Apr. 27, 2010), http://www.dankennedy.net/2010/04/27/more-on-the-haitian-copyright-case/.

154 Mark Cuban, Blog Maverick (March 29, 2009), http://blogmaverick.com/2009/03/29/are-tweets-copyrighted/.

155 The majority of tweets only relate facts or comments or retweet another's statement of fact. Kelly Ryan, ed. *Twitter Study Reveals Interesting Facts About usage*, San Antonio, Texas: Pear Analytics, (Aug. 12, 2009), http://www.pearanalytics.com/wp-content/uploads/2009/08/Twitter-Study-August-2009.pdf.

156 *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 499 U.S. 340 (1990).

157 *See Arica Institute, Inc. v. Palmer*, 970 F.2d 1067, 1072-73 (2d Cir. 1992).

158 *See Arvelo v. Am. Int'l Ins. Co.*, 1995 U.S. App. LEXIS 27165 (1st Cir. 1995) (per curiam) (citing Melville B. Nimmer & David Nimmer, Nimmer on Copyright, § 2.16, 185-85 (1995 ed.)).

159 Twitter Terms of Service, *available at* http://twitter.com/tos.

160 Creative Commons, About, http://creativecommons.org/about/.

161 Creative Commons, About, http://creativecommons.org/about/.

162 Creative Commons, What is CC? http://creativecommons.org/about/what-is-cc.

163 *See* http://creativecommons.org/.

164 Nine Inch Nails – The Slip download site, http://dl.nin.com/theslip/signup.

165 Nine Inch Nails – Remix page, http://remix.nin.com/.

166 United States Patent and Trademark Office, Copyright Basics, http://www.uspto.gov/web/offices/dcom/olia/copyright/basics.htm; Federal copyright law protects eight broad categories of original works: (1) literary works; (2) musical works; (3) dramatic works; (4) pantomimes and choreographic works; (5) pictorial, graphic, and sculptural works; (6) motion pictures and other audiovisual works; (7) sound recordings; and (8) architectural works. 17 U.S.C. § 102(a) (2001).

167 *Id.*

168 AdLaw by Request, Copyright (Dec. 22, 2004), *available at* http://www.adlawbyrequestlegacy.com/abr_knowledge_base/adlaw_resources.cfm?cit_id=1371&FAArea2=customWidgets.content_view_1&useCache=false&ocl_id=RESOURCE.

169 17 U.S.C. §§ 501, 106.

170 17 U.S.C. § 101; *MAI System Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993).

171 *Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2d 1453, 1458 (C.D. Cal. 2000).

172 *Castle Rock Entm't, Inc. v. Carol Publ'g Group, Inc.*, 150 F.3d 132, 144 (2d Cir. 1998).

173 *Id.* at 138.

174 *Nihon Keizai Shimbun, Inc. v. Comline Bus. Data Inc.*, 166 F.3d 65, 73 (2d Cir. 1999).

175 *Id.* at 71.

176 *Id.*

177 *Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2d 1453, 1458 (C.D. Cal. 2000).

178 17 U.S.C. § 107 (2001).

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

180 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/.

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

182 "The Commerce Department is playing catchup," Washington Internet Daily (Apr. 22, 2010).

183 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).

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

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

186 *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.

187 *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.

188 *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

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

190 http://www.cio.com/article/591831/Facebook_Privacy_Changes_5_Can_t_Miss_Facts?page=1&taxonomyId=3169

191 *Id*.

192 "Expansion triggers political backlash," Chicago Tribune, p. 27 (April 29, 2010).

193 http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_28_01_10_en.pdf

194 http://www.guardian.co.uk/technology/2009/dec/10/facebook-privacy

195 http://www.thesun.co.uk/sol/homepage/news/justice/article1398034.ece

196 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.

197 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.

198 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.

199 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.")

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

201 *Id.* at § 5.8.

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

203 *Id.* at §§ 8.6, 8.16.

204 http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf

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

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

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

208 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data implemented in the UK by the Data Protection Act 1998.

209 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).

210 http://www.guardian.co.uk/media/pda/2009/oct/30/digital-media-phorm

211 "Making privacy notices meaningful" The Reporter (Calleja Consulting) July 2009.

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

213 "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.).

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

215 http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm

216 http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html

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

218 "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).

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

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

221 See Harry Haydon The Sun dated 05 Jul 2009, available at http://www.thesun.co.uk/sol/homepage/news/2517719/MI6-spy-chief-has-cover-blown-on-Facebook-by-wife.html.; 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).

222 http://www.pcc.org.uk/news/index.html?article=NjA4MQ== ; "PCC Code – police comments sourced from private profiles on social networking sites" The Reporter (Calleja Consulting) December 2009

223 "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).

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

225 "Service via Twitter – the UK courts embrace technology" The Reporter (Calleja Consulting) November 2009

226 "FTC Tells Congress It Is Reviewing Whether Technology Changes Call for Revisions to the Agency's Rule Protecting Kids' Online Privacy," FTC website, http://www.ftc.gov/opa/2010/04/coppa1.shtm (April 29. 2010).

227 http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/?view=Binary The task force's good practice has now been integrated in to the work of the UK Council for Child Internet Safety.

228 http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

229 Whilst this may be based on a range of factors, there is an implication in the notes to the principles that a minimum age of 13 could be imposed in line with the U.S. approach and the Children's Online Privacy Protection Act which in the UK only allows providers to collect data without parental consent from users over 13 years old. Suggested measures to ensure age-appropriateness could include providing means for content providers, partners or users to label, rate or age restrict content when appropriate, using for example the Broadband Stakeholder Group's good practice principles on audiovisual content information.

230 For example, taking steps to ensure that private profiles of users registered as under 18 are not searchable.

231 http://ec.europa.eu/cyprus/news/20100209_safer_internet_en.htm

232 "Data protection offences – custodial sanctions" The Reporter (Calleja Consulting) November 2009; "Serious data protection breaches—civil monetary penalties" The Reporter (Calleja Consulting) December 2009.

233 See sections 4, 55, 55A and 55B of the Data Protection Act 1998 (as amended).

234 "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).

235 "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).

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

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

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

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

240 The authors wish to note the contributions of the following individuals to the content of this chapter: Samantha Clancy, Kimberly Craver, Nathalie Marchand, Michaela A. McCormack and Amber Spataro.

241 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.

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

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

244 http://www.independent.co.uk/news/media/current-twitter-trends-sun-ceo-tweets-his-resignation-modern-haikus-1889534.html.

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

246 Schedule 1(1) and Schedule 2(1) Data Protections Act 1998 htttp://www.statutelaw.gov.uk/legResults.aspx?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610.

247 Information Commissioner's Office (ICO) Employment Practice Code http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf.

248 ACAS Code of Practice http://www.acas.org.uk/index.aspx?articleid=2175.

249 French Labor Code, articles L. 1221-6, L. 1221-8, L. 1221-9, L. 2323-32.

250 This may be partly because of the inexistence of punitive damages in the French judicial system, which generally leads to a different approach to employment litigation than in some other jurisdictions.

251 The HALDE *("Haute Autorité de Lutte contre les Discriminations et pour l'Egalité")* is the administrative body that, among other things, assists employees in obtaining damages, or bringing actions before the relevant court regarding discrimination issues. Claims before the HALDE increased by 21 percent, to a total of 10,545 for 2009, compared with 2008. http://www.halde.fr.

252 This was the case when in 2008 the HALDE controversially carried out "testing" of major French companies, sending a number of fake CVs in response to job advertisements, and proceeded with a campaign of Naming and Shaming of those companies who statistically invited significantly less numbers of candidates from certain minority groups for interview.

253 La Commission nationale de l'informatique et des libertés, an independent French administrative authority whose mission is to ensure data privacy law is applied to the collection, storage, and use of personal data.

254 Such as the MEDEF (The Mouvement des Entreprises de France), employers' organization representing the French business leaders.

255 *"Charte réseaux sociaux, Internet, Vie Privée et Recrutement".*

256 An employee connected from home posted a comment on his personal Facebook page, criticizing his hierarchy. Two of his colleagues added other negative comments on to the post. All three were dismissed for gross misconduct. French judges will have to rule on whether such correspondence should be considered as private or not (and therefore, on whether or not it could be used, as grounds for dismissal).

257 Deloitte survey: 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.

258 Employers must be careful, however, to apply their computer policy consistently to avoid claims of discriminatory discipline and/or monitoring based on any protected category. For example, if the employer allows its employees to use social media sites, and in monitoring their usage discovers that certain employees are seeking to form a union, the employer may not focus its monitoring efforts on only the employees advocating for the union.

259 See *Blakley v. Continental Airlines, Inc.* 751 A.2d 538 (N.J. 2000)

260 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.

261 *See* Doe v. XYZ Corp., 887 A.2d. 1156 (N.J. Super. 2005).

262 16 CFR Part 255.

263 Information Commissioner's Office (ICO) Employment Practice Code, page 54 onwards http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf.

264 The relevant legislation in the UK is the Regulation of Investigatory Powers Act 2000 http://www.statutelaw.gov.uk/legResults.aspx?LegType=All%20Primary&PageNumber=3&BrowseLetter=R&NavFrom=1&activeTextDocId=1757378.

265 *Waters v Metropolitan Police Comr* [2000] IRLR 720.

266 http://www.theregister.co.uk/2008/10/23/sickie_woo.

267 Case No 06-45800 (Cass. soc., July 9, 2008): the employer is entitled to monitor its employees' Internet connections in the absence of the latter, given that connections during working hours, on the computer made available by the employer for the performance of the employee's work, are presumed to have a professional nature.

268 La Commission nationale de l'informatique et des libertés, an independent French administrative authority whose mission is to ensure data privacy law is applied to the collection, storage, and use of personal data.

269 Cases No 08-40.144 and 08-44.019 (Cass. soc., Feb. 3, 2010) An employer was held to be liable for the harassment that had occurred in the workplace despite having taken measures on becoming aware of the situation; in one case the perpetrator resigned and in another the victim of the harassment was moved to another site. Indeed, in such areas, employers are bound by an obligation to achieve a particular result "obligation de resultat" which is distinct in French contract and tort law from an "obligation de moyens," an obligation to act or a "best efforts obligation."

270 "*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").

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

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

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

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

275 See *Sigler v. Kobinsky*, 762 N.W.2d. 706 (Wisc. Appt. Ct. 2008); *Maypark v. Securitas Security Services USA, Inc*, 2009 WL 2750994 (Wisc. Appt. Ct. 2009).

276 *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).

277 National Labor Relations Act, 29 U.S.C. §§ 151-169.
Deloitte survey: 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.

278 la Cour de Cassation

279 Case n° 08-17.191 Cass. Soc., (Déc. 08, 2009). The information for internal use was not well enough defined to judge whether it was necessary and proportionate given the obvious breach of individual and collective rights and liberties, in this case

freedom of expression (based on article L. 1121-1 of the French labor code). Moreover, besides the consideration of civil liberties, the Labour Code contains specific articles (L. 2281-1 et seq.) pertaining to the employees' collective right to express themselves on issues such as working conditions and the content and organization of their work. The vague definition of information to be considered as confidential did include information on which employees may need to communicate. With regard to the whistleblowing disposition, employees were invited to denounce behavior thought to be in breach, not only of regulations pertaining to finance and fraud, etc., but basically of other regulations of the code of conduct as well. This was not strictly in line with the application of Sarbanes Oxley regulations and therefore infringed on employee rights. Moreover, the company did not comply with the proper CNIL procedure and was held as not providing enough protection to employees using the facility.

280 TGI Caen, (Nov. 5, 2009)

281 The authors wish to acknowledge the contributions of Areta L. Kupchyk to the content of this chapter.

282 Manhattan Research, Cybercitizen Health v8.0, *The State of eHealth: Trends of Today's eHealth Consumer*, at 203 (2008), available at http://www.ahdionline.org/ca/ahdi-wa/news/articles/The_State_of_eHealth.pdf.

283 *See generally*, 21 U.S.C. §§ 331(a) and 352(a), (n), (q) and (r).

284 Since May 2004, seven drug companies have paid a total of $7 billion in fines and penalties. In September 2009, one major drug company pleaded guilty to two felony counts of marketing an anti-inflammatory drug for unapproved uses and agreed to pay $1.19 billion (the largest criminal fine in U.S. history) and forfeit $105 million to the government. The company also agreed to pay $1 billion to resolve allegations under the False Claims Act that it illegally promoted the anti-inflammatory drug and three other drugs, and paid kickbacks to health care providers. In January 2009, another major drug company pleaded guilty and paid $1.42 billion in fines and penalties to settle charges that it had illegally marketed a drug approved for the treatment of schizophrenia. In September 2007, a third company paid $515 million—without admitting or denying wrongdoing—to resolve allegations of illegal drug marketing and pricing.

285 21 U.S.C. § 333(a)(1)-(2).

286 *See, e.g.,* 21 C.F.R. § 202.1.

287 *See* FDA, *Promotion of FDA-Regulated Medical Products on the Internet, Notice of Public Meeting*, 61 Fed. Reg. 48,707 (Sept. 16, 1996).

288 *See* The Pink Sheet (Nov. 8, 1999) pg. 22 (Statement of Melissa Moncavage, DDMAC Public Health Advisor, at Drug Information Association conference Oct. 23, 1999); *see also* DDMAC, Center for Drug Evaluation and Research presentation by Melissa Moncavage Nov. 3, 1999, at http://www.fda.gov/cder/ddmac/diammm1999/tsld003.htm.

289 For example, in November 2009, FDA's Office of Criminal Investigations (OCI), in conjunction with the Center for Drug Evaluation and Research, and the Office of Regulatory Affairs, Office of Enforcement, targeted 136 websites that appeared to be engaged in the illegal sale of unapproved or misbranded drugs to U.S. consumers. As part of this investigation, FDA issued 22 warning letters to the operators of these websites and notified Internet service providers and domain name registrars that the websites were selling products in violation of U.S. law. FDA, *FDA Issues 22 Warning Letters to Web site Operators—Part of International Internet Week of Action*, at http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm191330.htm.

290 *See* http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/UCM143487.pdf.

291 FDA Response to Ignite Health FDA Social Media, *Questions for the FDA Regarding 'Next Steps' for Guidance Related to the Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools*, Dec. 11, 2009, http://www.fdasm.com/docs/FINAL%20DDMAC%20Responses%20to%20FDASM_Questions.pdf.

292 *See* 74 Fed. Reg. 48083 (Sept. 21, 2009).

293 FDA Response to Ignite Health FDA Social Media, *Questions for the FDA Regarding 'Next Steps' for Guidance Related to the Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools*, Dec. 11, 2009, http://www.fdasm.com/docs/FINAL%20DDMAC%20Responses%20to%20FDASM_Questions.pdf.

294 FDA, *Guidance Agenda: New Draft Guidances CDER is Planning to Publish During Calendar Year 2010*, available at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm079647.pdf.

295 So long as the dissemination of off-label information is a scientific exchange between medical or science professionals, FDA will not consider it promotional; but if the dissemination is within a promotional context, FDA will regulate it as violative off-label advertising. Although the Internet, and social media specifically, may facilitate scientific discussions through interactive, immediate, and spontaneous exchanges in professional venues such as Sermo, FDA may consider discussions with multiple parties about off-label issues to be promotional in nature and not scientific exchange.

296 Promotional messages may not "recommend or suggest" the drug for unapproved uses. 21 C.F.R. § 202.1(e)(4)(i)(a). The only other thing more difficult than ensuring adequate advertising content is determining when a statement or activity is in fact promotional as opposed to scientific exchange. This is more important than it may appear at first blush. Technically, *any* statement or activity, from *anyone* – not just the company, its employees, vendors, or agents, but, anyone, so long as the company "knows, or has knowledge of the facts that would give [the company] notice – that suggests a use other than the specific use explicitly approved on the product label may be considered promotion of an unapproved or "off-label" use. 21 C.F.R. §§ 201.128 and 801.4. In other words, a company need not have any relationship with the person making the statement or conducting the activity; it need only have reason to know that the product is being used for an off-label purpose.

297 21 C.F.R. § 314.81 (b)(3)(i).

298 As background, the holder of an approved marketing application is required to "review all adverse drug experience information obtained *or otherwise received* by the applicant *from any source*, foreign or domestic, including information derived from

commercial marketing experience, postmarketing clinical investigations, postmarketing epidemiological/surveillance studies, reports in the scientific literature, and unpublished scientific papers." 21 C.F.R. § 314.80(b) (emphasis added). By participating in social media interactions, a company may be required to investigate every adverse event claim it comes across, regardless of its credibility. Such claims would also have to be reported if the company is able to determine at least four data elements: (1) an identifiable patient; (2) an identifiable reporter; (3) a specific drug or biologic involved in the event; and (4) an adverse event or fatal outcome. *Id.* FDA's current adverse event reporting guideline states that a company is relieved from the adverse event reporting obligation only if one or more of the four elements remain unknown "after being actively sought" by the company. *Id.* To what extent (if any) would this same standard apply to the Internet and social media communications is the question.

299 FDA, *Post-Approval Safety Data Management: Definitions and Standards for Expediting Reporting, ICH Harmonized Tripartite Guideline Draft* (July 18, 2003), available at http://www.fda.gov/RegulatoryInformation/Guidances/ucm129457.htm.

300 *DOD Report* April 2009, p. 33, available at http://www.usa.gov/webcontent/technology/other_tech.shtml.

301 *Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions*, Dec. 23, 2008, available at http://www.usa.gov/webcontent/technology/other_tech.shtml.

302 *Privacy and Government Contracts with Social Media Companies*, available at http://epic.org/privacy/socialnet/gsa/.

303 Carolyn and Peter appreciate the helpful comments of their Insurance Recovery Group colleagues Mark Hersh and Andrew Moss in the United States and Gregor Pryor in the UK in preparing this chapter.

304 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 that 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*, NAT'L UNDERWRITER, July 20, 2009.

305 *See* Eric J. Sinrod, *Data Security Breaches Cost Real Money*, TECHNOLOGIST, FINDLAW.COM, March 11, 2010, http://blogs.findlaw.com/technologist/2010/02/data-security-breaches-cost-real-money.html.

306 The authors wish to acknowledge the contributions of Maureen C. Cain to the content of this chapter.

307 *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

308 *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 http://www.nypost.com/seven/04202008/news/nationalnews/inside_youtube_divorce_107240.htm

309 *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); *Clark v. State,* 915 N.E.2d 126 (Ind. 2009) (affirming trial court's evidentiary ruling admitting boastful statements made by defendant on MySpace regarding how society labels him as an outlaw and criminal).

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

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

312 *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

313 The authors wish to acknowledge the contributions of Jesse J. Ash to the content of this chapter.

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

315 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).

316 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

317 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

318 In the Matter of Anthony Fields, Securities Act Release No. 9291 (January 4, 2012).

319 In the Matter of Michael Migliozzi II, Securities Act Release No. 9216 (June 8, 2011).

320 *See* FINRA, Quarterly Disciplinary Review (July 2011).

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

322 Case No. 10-CV-10406 (D. Mass. March 9, 2010).

323 Civil Action No. 08-CV-3859 (JES) (S.D.N.Y. April 24, 2008).
324 Civil Action No. CV09-231, (E.D. Tenn. Aug. 31, 2009).
325 The authors wish to acknowledge the contributions of Sachin Premnath to the content of this chapter.
326 Erik Schonfeld, *Nearly 75 million people visited Twitter's site in January* (16 February 2010), available at http://techcrunch.com/2010/02/16/twitter-75-million-people-january/
327 *Oneok, Inc. v. Twitter, Inc.*, Case Number 4:09-cv-00597 (N.D. Okl. Sept. 15, 2009).
328 http://www.guardian.co.uk/technology/2010/feb/05/vodafone-twitter-obscene-tweet
329 http://twitter.zendesk.com/forums/26257/entries/18367
330 http://en.wikipedia.org/wiki/Facebook
331 Sally M. Abel, "Trademarks and Rights of Publicity in the Converged World," 978 PLI/pat 57, September 2009.
332 http://www.facebook.com/legal/copyright.php?howto_report
333 http://www.facebook.com/terms.php?ref=pf
334 Allegations of copyright infringement are handled under the directive of the Digital Millennium Copyright Act, a separate form that is available to users.
335 15 U.S.C. §1114(1)(a).
336 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."
337 15 U.S.C. § 1125(c) liability against party who "at any time 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."
338 Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks.
339 s10, Trade Mark Act 1994
340 Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trademark.
341 *Céline Sarl v. Céline SA* (Case C-17/06)
342 *1-800 Flowers Inc. v. Phonenames Ltd* [2000] FSR 697
343 *Bundesgerichtshof* [German Federal Court of Justice], NJW 2005, p. 1435 – Hotel Maritime.
344 *Irvine v. Talksport* [2003] EWCA Civ 423
345 Sec. 4 no. 9 German Act Against Unfair Competition.
346 Cologne Civil Court, decision of September 16, 2009, file no. 33 O 374/08.
347 http://twitter.zendesk.com/forums/26257/entries/18366
348 *Id*.
349 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
350 *Anthony La Russa v. Twitter, Inc.*, Case Number CGC-09-488101 (Cal. Super. Ct., San Fran. Co., May 6, 2009).
351 *Bundesgerichtshof* [German Federal Court of Justice], NJW 2002, p. 2031 – shell.de; Hamm Court of Appeals, NJW-RR 1998, 909 – krupp.de.
352 http://twitter.com/help/verified
353 *Taser International Inc. v. Linden Research Inc.*, 2:09-cv-00811 (U.S.D.C., D. Ariz., April 17, 2009).
354 http://www.techdirt.com/articles/20090421/1310304599.shtml
355 http://www.bloomberg.com/apps/news?pid=20601103&sid=aR6xHcnBMn9M
356 *Adam Opel AG v. Autec AG* (Case C-48/05).
357 *Bundesgerichtshof* [German Federal Court of Justice], decision of January 14, 2010, file no. I ZR 88/08 (not yet published).
358 Nir Kossovsky, MISSION INTANGIBLE, Blog of the Intangible Asset Finance Society, September 21, 2009 (quoting Darren Cohen).
359 *Eros LLC v. Leatherwood*, No. 8:2007cv01158 (M.D. Fla. 2007).
360 *Eros LLC v. Simon*, Case No. 1:2007cv04447 (E.D.N.Y. 2007).
361 Registration No. 3,483,253 covering "providing temporary use of non-downloadable software for animating three-dimensional virtual characters."
362 Registration No. 3,222,158 covering "computer graphics services; graphic art design; graphic design services, graphic illustration serves for others."
363 Registration No. 3,531,683.
364 http://secondlife.com/corporate/tos.php
365 *Id*.
366 *Id*.
367 Abel, *supra* note 138.

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

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

370 This article is intended as a summary of the legal landscape and potential strategies for dealing with that landscape. However, nothing herein should be construed as a legal opinion or specific legal advice for a particular matter or situation.

371 For example, recent changes to 35 U.S.C. have made it more difficult to sue multiple defendants in a single case, and have provided alternative agency proceedings for challenging patents outside of civil litigation.