

# ReedSmith

The business of relationships.<sup>SM</sup>

## Network Interference: A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon

Third Edition

Twitter™

facebook®

BLOGGING

Trademarks

Meme

BRAND DILUTION

Employee Use

Virtual World

SECOND LIFE

**— PREFACE —****3<sup>rd</sup> 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 second edition added Europe.

This third edition is a major update and covers virtually every aspect of social media and the law on a global basis.

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.

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 Paul Matulac at [pmatulac@reedsmith.com](mailto:pmatulac@reedsmith.com)

Thank you.

Gregor Pryor  
Editor, Europe

Douglas J. Wood and Stacy Marcus  
Editors, United States

April 21, 2014

— EDITORS —

[Gregor Pryor](mailto:gpryor@reedsmith.com) - [gpryor@reedsmith.com](mailto:gpryor@reedsmith.com)

[Douglas J. Wood](mailto:dwood@reedsmith.com) - [dwood@reedsmith.com](mailto:dwood@reedsmith.com)

[Stacy K. Marcus](mailto:smarcus@reedsmith.com) - [smarcus@reedsmith.com](mailto:smarcus@reedsmith.com)

— TABLE OF CONTENTS —

Introduction..... 1  
Advertising & Marketing ..... 4  
Brand Protection & Reputational Management ..... 19  
Copyright (EU) ..... 33  
Copyright (U.S.) ..... 36  
Data Privacy & Security ..... 39  
Employment Practices ..... 50  
Food and Drug Administration..... 59  
Government Contracts & Investigations ..... 69  
Insurance Recovery..... 72  
Litigation, Evidence & Privilege ..... 77  
Product Liability..... 82  
Securities (UK) ..... 85  
Securities (U.S.) ..... 92  
Trademarks ..... 105  
The U.S. Patent Minefield..... 114  
Biographies of Authors and Editors ..... 118  
Guide to Social Media Terminology and Websites ..... 131  
Endnotes ..... 141



## 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, LinkedIn, YouTube, and Twitter. 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, YouTube channels, Twitter handles and much more. 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.<sup>1</sup>

### 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.<sup>2</sup>

### 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.”<sup>3</sup>

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. <sup>4</sup> 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.<sup>5</sup> The story was a lead story on CNN’s Situation Room, reported by anchor Wolf Blitzer.<sup>6</sup> As a result, United’s stock value fell considerably.<sup>7</sup> 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<sup>8</sup>, citing the United debacle.<sup>9</sup> 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.<sup>10</sup> Both traditional media and the blogosphere applauded his open communication and willingness to engage in a conversation about the problem.<sup>11</sup> 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.”<sup>12</sup>

## 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, Twitter, 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](http://www.adlawbyrequest.com)), and *Legal Bytes* ([www.legalbytes.com](http://www.legalbytes.com)).

It is no longer 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 Authors<sup>13</sup>

### United States

[Stacy K. Marcus](#), Partner – [smarcus@reedsmith.com](mailto:smarcus@reedsmith.com)

[Douglas J. Wood](#), Partner – [dwood@reedsmith.com](mailto:dwood@reedsmith.com)

[Frederick Lah](#), Associate – [flah@reedsmith.com](mailto:flah@reedsmith.com)

### United Kingdom

[Huw Morris](#), Associate – [hmorris@reedsmith.com](mailto:hmorris@reedsmith.com)

### Germany

[Stephan K. Rippert](#), Partner – [srippert@reedsmith.com](mailto:srippert@reedsmith.com)

[Katharina Weimer](#), Associate – [kweimer@reedsmith.com](mailto:kweimer@reedsmith.com)

[Alin Seegel](#), Associate – [aseegel@reedsmith.com](mailto:aseegel@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 and constantly-evolving 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 2.4 billion people use the Internet every day<sup>14</sup>, and, according to a 2012 study by Nielsen, people are continuing to spend more time on social networks than any other category of sites—20% of their time spent on PCs and 30% of their mobile time.<sup>15</sup> Combine that with the fact that smartphone ownership is over 64%<sup>16</sup> (with the percentage even higher in other parts of the world) and 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.<sup>17</sup> 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, a recent survey shows that 93% of marketers will be increasing or maintaining their spending on social media ads over the next year.<sup>18</sup> According to a 2012 study by eMarketer, social marketing spending already accounted for an average of about 6.6% of marketer budgets. Over the next five years, marketers expect social marketing spending to jump up to 15.8% of spending.<sup>19</sup> 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, viral videos, 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 presence on Facebook, Tumblr, Twitter, YouTube, or Pinterest, and are encouraging consumers to interact with their brand. Companies are increasingly using social media to provide customer service and get product reviews. According to a survey performed by The Connection, 47% of customers have sought customer service using social media, with the usage as high as 59% among 18-24 year olds. These high usage rates makes sense considering that 57% of customers search for a solution online first when they have a problem with a product.<sup>20</sup> Marketers seeking new ways to engage consumers have turned to social media as well, for example, to develop user-generated content ("UGC") around their brands for advertising on platforms like Instagram and Vine, and actively solicit their social networks to create buzz, viral and word-of-mouth advertising campaigns using hashtags and share plug-ins. Some, such as foursquare and Yelp, offer small rewards for consumers in exchange for "checking in" at a business. As newer platforms, like Snapchat, gain popularity, marketers will continue to find ways to transform consumer trends into new marketing channels. 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 to digital media. 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, monitors, tablets and smart phones. What once aired only on television is now being moved over to the Internet and new media 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 -American Federation of Television and Radio Artists ("SAG-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 on Facebook has more than 35.5 million fans and counting. The Starbucks YouTube channel has more than 22,000 subscribers and nearly 11 million upload views of videos. There are more than 1.7 million Starbucks followers on Instagram, over 1.6 million Starbucks followers on foursquare, and more than 5.4 million on Twitter. Don't forget Pinterest and Vine, with another 110,000 and 134,000 Starbucks followers, respectively. There's even a separate Facebook page dedicated to one of Starbucks' menu items, the Frappuccino, with nearly 11 million "Likes".

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, which serve as binding contracts, 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, Pinterest, Tumblr, Snapchat, and YouTube specifically prohibit use by children under the age of 13.<sup>21</sup> Facebook, YouTube, Twitter, Pinterest, Instagram, Snapchat, and Tumblr prohibit the repeated 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.<sup>22</sup> 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 Starbucks as an example, a search for "#starbucks" on Instagram currently yields nearly 7.5 million results and there are thousands of unofficial "Starbucks" pages and groups on Facebook. This is the current state of affairs. Facebook now requires that individuals registering a page agree to their Pages Terms, which says that "[a]ny user may create a Page to express support for or interest in a brand, entity (place or organization), or public figure, provided that it is not likely to be confused with an official Page or violate someone's rights."<sup>23</sup> Similarly, Tumblr, Pinterest and Twitter all have "Impersonation Policies" that prohibit "accounts that mislead or deceive others" and "non-parody impersonation."<sup>24</sup>

Despite these efforts by social media platforms such as Facebook, Instagram, YouTube, Tumblr, Pinterest, 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 hundreds of "I love Starbucks" pages and groups. If a consumer cares for a Frappuccino, 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 or "Starbucks sucks" page. 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](http://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 localised pages for several countries, including Germany, Indonesia, Mexico and South Africa. The discussion board on the page not only deals with maintenance and repair issues has moved to showcasing more fashionable topics such as Louis Vuitton branded tailor-made luggage for BMW cars. BMW also asks its users to vote on polls and gives them the opportunity to showcase their loved ones. All-time competitor Mercedes Benz has changed its Facebook page to allowing fans to post on the Mercedes' wall (previously not possible). Like BMW, Mercedes posts updates relating to new models and to topics related to Mercedes that enhance the brand's image in the online world, such as Formula 1 wins or placements. Mercedes also hosts an official Facebook page for the popular AMG cars, while manufacturer Porsche places a much stronger emphasis still on racing results. 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. Porsche even permits 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. However, the "legal awareness" has risen – BMW's and Mercedes' pages have an imprint (a requirement for telemedia services provider under German law), Porsche even provides website terms of use.

The legal aspects of these brand interactions do not differ materially from the issues raised under U.S. and UK 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 sensitivities.

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. In fact, Instagram has recently developed a page solely dedicated for this purpose, “Host a Photo Campaign,” which provides helpful tips on how to host a successful photo contest on Instagram and cites numerous successful examples, including General Electric, Brisk Iced Tea, Charity Water, and NBC News.<sup>25</sup> Twitter has also become one of the most popular platforms for promotions. Some often examples include giveaways for the first 10 people to re-Tweet a Tweet to the first to correctly answer a trivia question to the “most creative” Tweet in response to a question. As a result of its popularity, Twitter has posted guidelines for contests and sweepstakes on Twitter to help make sure the contests and sweepstakes do not violate Twitter’s other terms, though they are far less rigorous than Facebook’s and simply serve as guidance, rather than binding terms.<sup>26</sup> Facebook’s terms of service also set forth a number of requirements for businesses who use the platform to run a sweepstakes and promotion. The Pages Terms express state the business is responsible for the lawful operation of that promotion, including: (a) the official rules; (b) offer terms and eligibility requirements (ex: age and residency restrictions); and (c) compliance with applicable rules and regulations governing the promotion and all prizes offered (ex: registration and obtaining necessary regulatory approvals). Facebook further requires that promotions include a “complete release of Facebook by each entrant or participant” and “[a]cknowledgement that the promotion is in no way sponsored, endorsed or administered by, or associated with Facebook.”<sup>27</sup>

As the number of promotions on Facebook increased, Facebook revised its Promotion Guidelines in August 2013 to make it easier for businesses to create and administer promotions by removing the requirement that promotions on Facebook only be administered through apps (previously business were not permitted to administer promotions on personal timelines). Now, businesses are able to: (1) collect entries by having users post on the Page or comment or “Like” a Page post; (2) collect entries by having users message the Page; and (3) utilize “Likes” as a voting mechanism.<sup>28</sup> Twitter and Pinterest have also developed guidelines for businesses administering promotions on their platforms.<sup>29</sup>

Other companies have taken their contests off of a particular social media platform and instead operate a contest-specific microsite, often in coordination with companies specializing in social media promotions, such as Votigo, Wildfire and Strutta,. One such brand is Frito Lay’s Doritos, who for several years has sponsored a well-known Super Bowl contest, encouraging people to submit their own Doritos commercial on a dedicated URL, while encouraging users to share their submissions via social media.<sup>30</sup> The winning commercials are then aired during the Super Bowl. The 2013 version of the contest is especially interesting as one of the winners also receives the opportunity to work with Marvel on the next “Avengers” movie; the other winner receive \$1 million. 2013 also marked the first time people outside of the U.S. were permitted to participate – in fact, the contest was open to entrants from 46 countries. Folgers has been administering a similar social media contest on a dedicated URL which encourages people to submit their take on the iconic jingle, “The Best Part of Wakin’ Up” (*See “User-Generated Content” below for issues relating to UGC*).<sup>31</sup> 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 in social media-based promotions like the ones held by Doritos and Folgers. What if the winner (or performers featured in 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?

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. Some companies address this issue by developing a geo-fenced microsite with an API for the applicable social media platform, which (hopefully) prevents entrants from outside the eligible territory. This represents both an opportunity and a challenge—both fraught with legal and regulatory possibilities.

In the United States<sup>32</sup>, 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<sup>33</sup>). 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.<sup>34</sup> 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.<sup>35</sup>

### 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

#### Influencers and Native Ads

##### United States

“People are either going to talk with you or about you.”<sup>36</sup>

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 (*See Chapter 2 – Commercial Litigation*). Some examples include offering small rewards (e.g., discounts) at businesses for “checking-in”, including customized hashtags in posts, offering share plug-ins on the advertiser’s site, using third-party reviewers (e.g., influencers) to create product reviews, offering giveaways on third-party sites or creating a company-sponsored blog (*see “Customer Service and Customer Feedback” below*).

Companies often provide products to influencers so that they can write a (hoped-for favourable) review of the product. For example, a New York Times blog investigated a tweet by pop singer Miley Cyrus to her 12 million followers, thanking a private jet company for a flight.<sup>37</sup> Although Ms. Cyrus declined to comment, the company admitted that she was given some consideration for her tweet. Nowadays, it is becoming increasingly unclear to consumers whether celebrities are genuinely plugging a product they admire or if they are just paid to tweet about it.

While this practice is generally acceptable, provided that the reviews are legitimate, companies who fail to disclose the connection between influencer and company may face regulatory scrutiny and consumer backlash. Part of the regulatory concern is that unless the company discloses the material connection, consumers will have no way of knowing whether the reviews are real or artificial. In September 2013, the Harvard Business Review released a study that showed that many businesses that do not have a good reputation online will in fact try to create one by submitting fake reviews to web sites, such as Yelp.<sup>38</sup> As a result, some companies, such as Yelp, have implemented measures to combat fake reviews, including by utilizing a filtering algorithm and by posting consumer alerts on business listings that write fake reviews.<sup>39</sup>

The desire to have favorable online reviews has driven some companies to seek out and hire reputation-enhancement firms to write fake positive reviews on sites like Google and Yelp, a practice often referred to as “astroturfing.” In September 13, 2013, the New York Attorney General concluded a year-long investigation into the manipulation of consumer-review websites, which resulted in fining 19 firms a total of \$350,000 for engaging in the practice.<sup>40</sup> Part of the Attorney General’s operation, which went by the name of “Operation Clean Turf,” involved setting up a fake yogurt shop in Brooklyn that was seeking to combat negative reviews online. The Attorney General found that the reputation enhancement companies

who offered to assist the fake yogurt shop violated multiple state laws against false advertising and engaged in deceptive business practices.

Federal regulators are paying attention to these issues as well, particularly with respect to the need to disclose material connections. In 2009, the Federal Trade Commission ("FTC") revised its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* (the "FTC Guides").<sup>41</sup> 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."<sup>42</sup> Later, in March 2013, the FTC reminded advertisers again to disclose such material connections in its revised guidance for Dot com Disclosures.<sup>43</sup>

In sum, a company that provides products to a influencer for purposes of a product review should never instruct the influencer regarding what to say in the review, or ask to edit the material substance of review prior to posting. While companies should provide influencers 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 influencers for future reviews. The company should also caution its personnel about engaging in inflammatory disputes with influencers ("flaming") on any review or community-based sites. In addition, since under the FTC Guides a company could be liable for claims made by an influencer, the company should monitor product reviews made by influencers to ensure that the claims made are truthful and can be substantiated.

Another strategy to help marketers influence the conversation about their brands is native advertising. "Native advertising" refers to when an advertiser blends ads as editorial content to market more seamlessly. The Huffington Post was one of the first publications to utilize native advertising, when it teamed up with IBM to create technology-based content.<sup>44</sup> Other sites like BuzzFeed, TheOnion.com, and College Humor all feature content that look just like any other post, but are actually paid advertisements.

While native advertising can result in less intrusive marketing and brand association with an experience, the downside is that the blurring of content can, in some

instances, lead to misleading consumers. Advertisers should disclose the sponsorship or endorsement relationship clearly and conspicuously. The FTC has made the issue of native advertising one of increasing agency interest, with recent updates to its Search Engine Advertising guidance, Dot com Disclosures, and Endorsement guides all addressing potential issues with native advertising. In addition, sites that employ native advertising can run into content maintenance issues. Just ask The Atlantic. After allowing the Church of Scientology to post sponsored content on The Atlantic website, some readers criticized the media company for the content. Some readers called the content "bizarre" and "blatant propaganda."<sup>45</sup> Two weeks after the incident, The Atlantic posted new advertising guidelines to address native advertising.<sup>46</sup>

#### *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 reviewer 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 reviewer copies content for the 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 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 reviewers perceived this behaviour as contravening an unwritten reviewer's code of ethics (and indeed review site operators are looking for ways of prohibiting unwanted advertising activities on their sites), 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 review site operators the amount saved by avoiding the traditional booking of advertising space on the site or surrounding the site. Comparable decisions have been made with regard to the unauthorised use of photographs. However, court decisions on advertisement on review sites have not reached the press...yet.

### *Customer Service and Customer Feedback*

Online reviews also foster customer feedback and engagement with a brand. General Motors, for example, has a a blog called the Fast Lane which helps to foster engagement.<sup>47</sup> 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."<sup>48</sup> Fast Lane, of course, links 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."<sup>49</sup>

Once you've started the conversation, you can use social media to provide nearly instantaneous customer service and receive customer feedback. Many companies now provide customer service via Twitter. American Express, for example, has set up a dedicated Twitter handle to field customer care questions, to go along with its various other social media accounts on Facebook, Twitter, and YouTube.<sup>50</sup> GoDaddy, as another example, has a dedicated social media team and provides live technical support and best practice tips on Twitter.<sup>51</sup> Other companies like Southwest Airlines, Citi and eHarmony offer similar support services on their social media accounts. Many other companies also hold live Q&A sessions and polls on Twitter and other platforms. Think kids say the darndest things? Wait until you see what customers say once they start talking.

A major fast food restaurant launched a Twitter campaign as a way to promote the brand's food through good-natured, heart-felt stories using a specific hashtag. Instead, the Twitter-verse used it as an unsolicited opportunity to bash the restaurant. Oops, now what? While the company quickly pulled the campaign, such customer feedback-based campaigns can be hard to control. The hashtag continued to trend even after the campaign was pulled. In another example, a major retailer launched a campaign in 2012 in cooperation with a famous rapper. As part of the promotion, the rapper agreed to visit whichever retailer location generated the most Facebook likes. One writer saw this as an opportunity to pull off a prank on the rapper by creating a Facebook page dedicated to sending him to the retailer's Kodiak, Alaska's location. Through the power of social media, 70,000 users ended up liking the Kodiak, Alaska location's page, despite the fact the town only boasts a population of 6,200. Nonetheless, the rapper graciously showed up and performed at the retailer's Kodiak, Alaska location.

Still doubt the power of social media? The past year has been full of social media horror stories from companies, and perhaps no social media platform has served as a reminder about the dangers of social media than Twitter. In September 2013, fashion designer Kenneth Cole drew criticism for his controversial Tweet about the Syrian war: "'Boots on the ground' or not, let's not forget about sandals, pumps and loafers. # Footwear." The negative reaction the Tweet drew caused the designer to delete the Tweet, apologize, and issue a formal statement through a spokesperson. In another example, in June 2013,

outspoken, conservative Chick-fil-A president Dan Cathy spoke out against gay marriage on Twitter, only to delete the tweet shortly after. By that time, though, it was already too late as several Twitter users took screenshots and shared the tweet. Chick-fil-A released a public statement explaining why the tweet was taken down, however that did stop public protests resulting at some of franchise's restaurants. The restaurant later released a statement saying it did not intend to engage in political and social debate. And perhaps the biggest faux pas came in December 2013 from (of all people) the head of corporate communications for media company IAC, Justine Sacco. Prior to her trip to South Africa, Sacco infamously tweeted, "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!" Her attempts to delete the Tweet and her entire account were futile. Despite having less than 500 followers at the time, Sacco's Tweet went viral in no time. Soon thereafter, she was fired. Who knew 140 characters could get people and their companies into so much trouble?

A common culprit in a social media debacle is the result of an employee mistakenly posting from the corporate account, rather than his or her personal account. Such was the case back in 2011, when an employee from Chrysler's digital agency, New Media Strategies, tweeted from the @ChryslerAutos account: "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to [expletive] drive." Although the tweet was quickly deleted, the tweet had already spread to blogs. Chrysler decided not to renew its contract with New Media Strategies two days after the tweet.

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 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 post? Was it a third-party commenter on a page? 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 page, the

company, has the right to remove any posting it desires, subject, of course, to its policies and the terms on which the page is made available. Where comments are made on a third-party's page, a company could attempt to contact the author of the page and seek removal of the post. However, depending upon the content of the post, it may not be in the company's best interest to take it down.

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

### *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).

Crowdsourcing, which refers to the practice of obtaining services or content from the online community, for example, has been an increasingly utilized strategy by marketers. We previously mentioned the Frito Lay's Doritos Super Bowl commercial campaign. In addition, in 2013, Frito Lay also conducted its "Do Us A Flavor" contest which asked consumers to submit their ideas for a new flavor of Lay's potato chips.<sup>52</sup> After garnering nearly 3.8 million consumer-generated flavor submissions, the submissions were narrowed down to three finalist flavors. With more than a million votes cast on Facebook, Twitter, and text, the next flavor— Cheesy Garlic Bread— was selected. The grand prize winner was awarded \$1 million in cash. Not too bad for a bag of chips. Other marketers like Samuel Adams and Arizona Iced Tea have also sought public input to create new product flavors. With the popularity of crowdsourcing on the rise, companies like Tongal and Poptent have surfaced, providing content creators with a platform to share their work and connect with others.

While offering consumers to ability to submit their own UGC through crowdsourcing, there are also accompanying

risks with respect to intellectual property and false advertising. It's a mistake to think that, "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. In 2007, in what was a first-of-its-kind case, Subway filed a lawsuit against Quiznos<sup>53</sup> 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. The lawsuit claimed 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.<sup>54</sup> Nearly three years later, on February 23, 2010, following the court's denial of its motion for summary judgment, Quiznos agreed to settle the dispute.

In 2013, the proprietor of a hotel brought a defamation suit against TripAdvisor after his hotel was voted by users on its annual "Dirtiest Hotels list."<sup>55</sup> The proprietor alleged that TripAdvisor destroyed the hotel's business by publishing the user-generated comments, and that the list was based on distorted ratings and misleading statements. Nonetheless, the court found that the proprietor did not state a plausible claim for defamation against TripAdvisor because the list was based on the subjective views of its users, not an objectively verifiable fact. Readers of the list, according to the court, would understand the list published by TripAdvisor to be communicating subjective opinions of travelers who use TripAdvisor, which amounted to nothing more than hyperbole.

Following the court's decision in these two cases, 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, Instagram, Vine, 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 social media platform providers, 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. This is especially true in light of the fact more and more retailers are using photos from every day consumers from platforms like Instagram, as reported in the Wall Street Journal in May 2013.<sup>56</sup> Despite this increasingly prevalent practice, though, the legal risk of using an individual's content without his or her express permission is very real. For example, in January 2013, a U.S. federal court ruled that Getty Images and Agence France-Presse, a news agency, were liable for infringement for posting and distributing a photojournalist's images he posted on Twitter of the 2010 Haiti earthquake, without his permission. Months later, the court ordered the defendants to pay the photojournalist \$1.2 million in statutory penalties.<sup>57</sup> A similar lawsuit was brought by another photographer in June 2013 against BuzzFeed for the use of an image it found on Flickr.<sup>58</sup> 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.

In a more recent example, a nationwide class action was brought against Facebook in connection with one of its advertising programs called "Sponsored Stories." "Sponsored Stories" displayed a user's "Like" in connection with the user's name and profile picture to try to convince the user's friends to similarly "Like" the brand. Advertisers paid Facebook for these "Sponsored Stories"

advertisements. A class action was brought against Facebook in California federal court, alleging that Facebook misappropriated their names, profile photos, and likenesses in paid advertisements without their consent. In denying Facebook's motion to dismiss, the court held that plaintiffs – even non-celebrities -- could claim economic injury when their likeness is shared among people without their consent. The parties eventually reached a settlement, which was given final approval by the court in August 2013.

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-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 decision of the German Supreme Court<sup>59</sup> 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](http://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 Supreme Court established several criteria which could

lead to the assumption that UGC will be considered as a company's content: • extensive granting of rights of use regarding the UGC in favor of the company, • company's statement that UGC is checked before activation, • no indication of UGC as such. 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, in particular with regard to rights ownership. To the extent copyrighted materials are involved in the UGC, it is not possible to exclude monetary compensation for the use of the copyrighted materials, even if the user who provided the content agrees to such exclusion. He/she is permitted to claim "appropriate" compensation afterwards, e.g. in cases where certain UGC becomes famous and important for the company who uses it.

Related to the problem area "liability for UGC" is the question whether the website provider infringes third party rights in case of embedding infringing content on his website by "framing". Amongst German case law and literature that question is at issue. The German Supreme Court decided that framing is not subject to the right of making works available to the public according to Section 19 a German Copyright Act. However the German Supreme Court submitted that question at issue to the European Court of Justice<sup>60</sup> due to the construction of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. In particular the German Supreme Court wants to know whether framing is subject to the right of communication to the public of works and right of making available to the public other subject-matter according to Section 3 of the aforementioned directive. The decision of the European Court of Justice is expected in the course of 2014.

**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. Those terms and conditions should not contain an extensive grant of rights of use regarding the UGC in your favor and furthermore you should not state that UGC is checked by you.

**Talent Compensation**

**Commercial or Content?**

*United States*

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 SAG-AFTRA, as well as musicians under a contract with the American Federation of Musicians (“AFM”).<sup>61</sup> 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, such as Instagram videos, Vine videos, and Flipagram. 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 Commercials Contract applies 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 Commercials Contract and the advertiser is not obligated to compensate performers in accordance therewith and can negotiate freely for appropriate terms. “New Media” is defined as “digital, electronic or any other type of delivery platform including, but not limited to, commercials delivered to mobile phones and other digital and electronic media. The term New Media is intended to be all inclusive of digital, electronic or any other type of delivery platform whether no known or unknown.” Increasingly, the lines between television, Internet and New Media are blurred, as consumers access traditional TV programming on computers, tablets and smartphones. What remains clear, however, is that 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”).

The Commercials Contract provides for minimum levels of compensation, depending upon the length of use for the spot for both Made Fors and Move Overs. For eight weeks or less, performers must be paid 133 percent of the applicable session fee for a Made For and 150% of the applicable session fee for a Move Over. For a one-year cycle, payment equals 350 percent of such fee for a Made For and 400% for a Move Over.

**New Digital Provisions of the Commercials Contract**

In 2013, the JPC negotiated groundbreaking improvements to the SAG-AFTRA Commercials Codes in the area of Internet and New Media. Specifically, the JPC negotiated the carveout of four types of commercials from coverage under the Commercials Codes: user-generated/crowdsourced commercial contests, live events commercials, hidden camera commercials, and man on the street commercials. With respect to these areas, producers no longer have to worry whether the content is or is not a “commercial”. Instead, they are free to produce the commercial (subject to the terms set forth below) without paying for the commercial under the SAG-AFTRA Commercial Codes and without hiring union performers.

**User-Generated/Crowd-Sourced Commercial Contests:** Producers may now solicit, accept and display via the

Internet user-generated/crowd-sourced commercials as entries to a contest.

- a. Such contest entries may be exhibited via the Internet during the contest period without triggering any application of the Commercial Codes including, without limitation, Ad Lib or Creative Session Call fees for the entry.
- b. If a contest-winning commercial is exhibited on any media platform after the expiration of the contest period, such commercial will be subject to the rates, terms and conditions of the Commercial Codes.
- c. Non-winning contest entries must be pulled down from the Internet or New Media upon declaration of the winner. Should Producer choose not to cease exhibition of the non-winning entries, such entries will be subject to the rates, terms and conditions of the Commercial Codes.

A Producer may film or record activities of persons in public without covering such persons under the Contract, provided such persons are neither scripted to speak any dialogue nor cast for the commercial(s), as follows:

- a. **Live Events** – “Live Events” are events attended by at least 20 persons who are neither hired nor cast by Producer to attend the event. An individual(s) appearing in such footage will not be a Covered Person(s) for purposes of the Commercial Codes. However, such Live Events (1) may not be staged for the purpose of producing a commercial(s); and (2) non-covered participants at the live event may not receive individual direction but may be directed as a group.
- b. **Man on the Street Commercial** – A “Man on the Street Commercial” means a commercial(s) where an interviewer interviews people on the street, at public venues, or at live events and asks them questions or makes statements or gestures to elicit a response or reaction from them. An individual(s) appearing in such footage will not be a Covered Person(s) for purposes of the Commercial Codes. The interviewer is a Covered Person for purposes of the Commercial Codes whether or not they appear or perform in the commercial(s).
- c. **Hidden Camera Commercials** – A “Hidden Camera Commercial” means a commercial(s) comprised of footage captured by a hidden camera(s) without direction to the individual(s) being filmed. An individual(s) appearing in such footage will not be a

Covered Person(s) for purposes of the Commercial Codes. Any person(s) appearing in the capacity of an interviewer, however, will be a Covered Person whether or not they appear in the commercial.

As a condition of the waiver, Producer must notify SAG-AFTRA that it has used the waiver and provide SAG-AFTRA with an electronic or physical copy of the commercial(s) within 60 days of the first exhibition of the commercial.

If a commercial produced pursuant to this waiver is subsequently exhibited other than on the Internet or New Media where such use is otherwise covered by the Commercial Codes, anyone qualifying as a principal in the commercial as subsequently exhibited will be a Covered Person under the Commercial Codes and compensated accordingly.

The addition of these provisions provides added flexibility to signatory producers working in digital media.

**Unauthorized Use**

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)? Is the advertiser obligated to pay the actors under the Commercials Contract for use of the commercial that was not authorized by the advertiser? 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. This was a fertile area for disagreement between the advertising industry and the unions. In 2011, however, SAG-AFTRA have confirmed that there is no requirement in the Commercials Contract for a signatory to issue a take down notice in response to a claim of unauthorized Internet use on, e.g., You Tube. However, if signatories elect to cooperate and send a take down notice, such cooperation will not be considered by the union to be evidence of an accepted industry practice under the Commercials Contract. Further, the sending of a take down notice in response to a claim of unauthorized Internet use will not be used precedent. Meaning, if a signatory sends a take down notice in response to one specific request from the unions, this does not mean that a signatory is then obligated to send a take down notice in response to any or all future requests.

## 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*

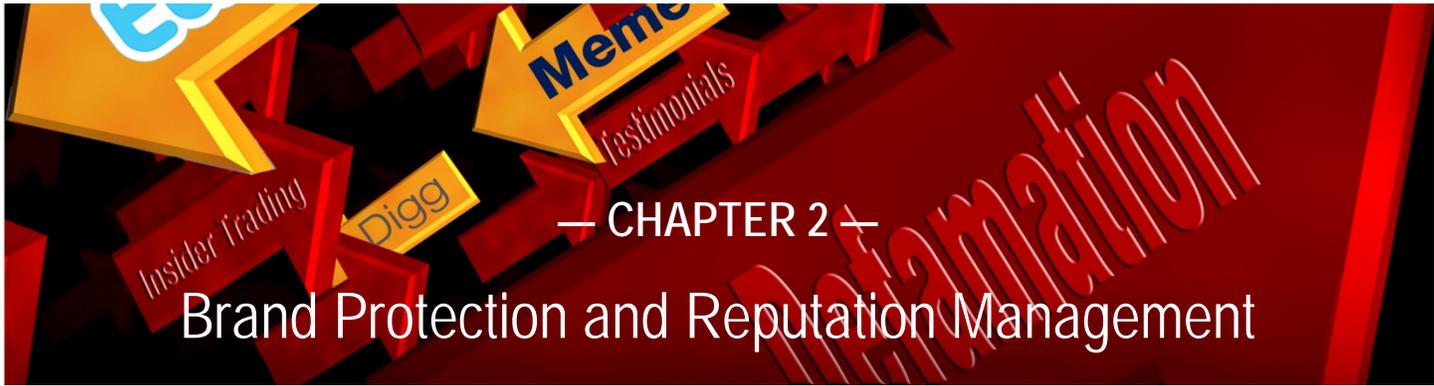
The Directive 2006/114/EC dated 12 December 2006 regulates misleading and comparative advertising; the Directive 2005/29/EU dated 11 May 2005 regulates unfair business-to-consumer commercial practices.

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 Authors<sup>62</sup>

### United States

[Peter D. Raymond](#), Partner – [praymond@reedsmith.com](mailto:praymond@reedsmith.com)

[David A. Scharfstein](#), Associate – [dscharfstein@reedsmith.com](mailto:dscharfstein@reedsmith.com)

### United Kingdom

[Emma Lenthall](#), Partner – [elenthall@reedsmith.com](mailto:elenthall@reedsmith.com)

[Louise Berg](#), Senior Associate – [lberg@reedsmith.com](mailto: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.<sup>63</sup> 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.<sup>64</sup>

### ***False Advertising Generally***

Generally, the tapestry of laws covering false advertising consists of Section 5 of the FTC Act<sup>65</sup> (the “FTC Act”), Section 43(a) of the Lanham Act,<sup>66</sup> 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.”<sup>67</sup> Actions under the FTC Act may only be asserted by the FTC; there is no private right of action under this Act. According to the FTC Policy Statement on Deception (1983),<sup>68</sup> 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 than actual evidence in the marketplace.<sup>69</sup> 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.<sup>70</sup> The advertiser generally bears the burden of substantiating the advertising claim.<sup>71</sup> The FTC Act permits monetary and injunctive relief.<sup>72</sup>

### ***Private Rights of Action***

#### *The National Advertising Division*

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.

#### *Section 43(a) of The Lanham Act*

Competitors are also protected against deceptive practices under Section 43(a) of the Lanham Act, which provides for civil actions for injunctive and monetary relief (in state or federal court) for false or misleading statements made in

commercial advertisements. 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.<sup>73</sup> 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.<sup>74</sup> 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.<sup>75</sup> In cases of implied deception, this means the plaintiff will have to introduce extrinsic consumer survey evidence.

### ***State Court Claims and Class-Action Lawsuits***

In addition to FTC, Lanham Act, and NAD claims, advertisers must be mindful of the threat of claims asserted under the various state consumer deception laws, and *particularly* mindful of the potential for class-action suits under these statutes. In fact, as a practical matter, a determination of liability by the FTC, NAD, or a federal court is often a precursor to a class-action suit, as plaintiffs (and plaintiffs’ attorneys) utilize the prior finding of liability to bolster their claims that the allegedly false or misleading advertisement caused damages to the entire class of individuals who were exposed to it.<sup>76</sup>

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.<sup>77</sup>

### ***“Word of Mouth” Marketing***

#### *The Duty to Disclose*

Social media has spawned a new advertising industry that spreads brand messaging in an old-fashioned way: word-of-mouth. 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.”<sup>78</sup>

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.<sup>79</sup> 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?”<sup>80</sup>

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.<sup>81</sup> 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.<sup>82</sup> 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*):<sup>83</sup>

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.”<sup>84</sup>

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.”<sup>85</sup> 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.”<sup>86</sup>

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.”<sup>87</sup> Again, that relationship may exist with otherwise remote users. The FTC points out, however, that “[i]t, 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.<sup>88</sup> To avoid prosecution, if not liability, advertisers should heed the Commission's admonition:<sup>89</sup>

[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:<sup>90</sup>

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

...

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

*Word of Mouth Marketing: Summary*

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

*Recent Developments in Social Media Advertising Law*

In March, 2013, the FTC released a revised version of its so-called “.com Disclosures,” which provides “information that businesses should consider as they develop ads for online media...”<sup>91</sup> and was last published in 2000. The Disclosures reaffirm the FTC's position that consumer protection laws apply equally to all commercial activities regardless of the medium on which they appear, including on mobile and other space-constrained platforms like Twitter. Therefore, advertisements, endorsements, and other promotional communications that would be accompanied by disclosures in traditional media must be accompanied by equivalent disclosures in space-constrained media, and “if a particular platform does not provide an opportunity to make clear and conspicuous disclosures, then that platform should not be used to disseminate advertisements that require disclosures.”<sup>92</sup> In one of the examples provided in the Disclosures, the FTC suggests that placing the text “Ad:” before an endorsed tweet promoting a weight-loss product may sufficiently disclose the promotional nature of the tweet, and placing the text “Typical loss: 1lb/wk” may sufficiently disclose that the results described in the tweet (“30lbs in 6 wks”) were not typical.<sup>93</sup>

As advertisers continue to integrate their promotional messages into social media, the issues discussed in the .com Disclosures are likely to be the subject of a great deal of litigation. In fact, in August, 2013, the actress Octavia

Spencer filed suit against the manufacturer of a weight-loss product named Sensa, after Sensa allegedly terminated her promotional contract because she insisted upon placing the hashtag "#spon" after her sponsored tweets.<sup>94</sup> As of the time of this writing, the case is currently pending before the Los Angeles Superior Court.

Another emerging trend associated with the advent of social media is that false endorsement cases – which arise under Section 43(a) of the Lanham Act and have traditionally involved claims that a celebrity or other famous person's name or likeness has been used improperly to promote particular goods or services – are increasingly being filed by non-celebrity plaintiffs.<sup>95</sup>

In *Doe v. Friendfinder Network, Inc.*, for example, 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 – "petra03755" – in one of defendant's communities that contained nude photographs of the plaintiff and representations that she engaged 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 the 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:

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' Code of Advertising Practice (CAP Code).<sup>96</sup> While this Code only applies at present to advertisements in 'paid for' space, advertisers' own marketing communications on their own websites and in other non-paid-for space online under their control, such as their Facebook page or YouTube channel, this may change in the future. There is political pressure to extend the remit of the ASA and the CAP Code to all promotional messages on the Internet.

The ASA will not regulate any advertisements published in foreign media or which originate from outside the UK. 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 or misleading 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, sanctions 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 for direct mail advertisers)
- Enforced pre-publication vetting for repeat offenders

- Ineligibility for industry awards for repeat offenders
- 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 ("OFT"). The OFT can seek undertakings or an injunction through the courts or issue an Enforcement Order under the Enterprise Act 2002 (although it should be noted that current planned reforms to consumer rights legislation will abolish the OFT in April 2014 and merge its enforcement functions into Trading Standards).

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.

It should be noted that the ASA does not automatically intend to stamp out anything which pushes the boundaries. The Codes are often subject to interpretation and the ASA often surprises the industry with its decisions. As an example, the UK Home Office displayed posters on the side of vans driven through London, featuring a close-up image of someone holding a pair of handcuffs and wearing a uniform with a badge which stated "Home Office". The text stated "In the UK illegally?" and "106 ARRESTS LAST WEEK IN YOUR AREA\*". Underneath, text stated "GO HOME OR FACE ARREST Text HOME to XXXXX for free advice, and help with travel documents". Complainants challenged whether the phrase "GO HOME", was offensive and distressing, because it was reminiscent of slogans used by racist groups to attack immigrants in the past. The ASA stated that it considered that, in context, the claim would be interpreted as a message regarding the immigration status of those in the country illegally, which was not related to their race or ethnicity. The ASA recognized that some aspects of the poster were likely to be distasteful to some in the context of an ad addressed to illegal immigrants but concluded that the poster was unlikely to cause serious or widespread offence or distress and it was clearly addressed to illegal immigrants rather than to non-naturalized immigrants who were in the UK legally or to UK citizens. Those parts of the investigation relating to causing serious or widespread offence were not upheld. Likewise, advertisements for various charities have been very hard-hitting and have caused distress resulting in high numbers of complaints from the public, yet the ASA has chosen not to uphold these complaints. Perhaps the ASA believes that some issues are so important that it gives an extra degree of latitude. For example, a harrowing advertisement for the children's charity Barnardo's a few

years ago, received almost 500 complaints from the British public, yet the ASA said that the imagery was justified because the purpose of the ad was to raise awareness of the impact of domestic child abuse. However, the ASA has recently indicated that its approach to shock-inducing charity advertising may not be as lenient in the future. In 2013, it published a report asking "Are we being too charitable?"<sup>97</sup> and launched an investigation into the issue. We will see the results of this investigation, and potentially some guidance on the issue, during the course of 2014.

**False Endorsements**

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. As always, the endorsement must be true and in no way misleading.

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 and other forms of “native advertising” 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. The regulations should also be adhered to by advertisers using celebrity endorsements on social media, where it isn’t clear that the celebrity is being paid to advertise the relevant products/services. As we will discuss later in this White Paper, the ASA has recently suggested the use of key words and hash-tags to indicate beyond a shadow of a doubt such paid-for endorsement activities.

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. 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.”<sup>98</sup> 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, statements of opinion are generally not held to be defamatory, but the lines between opinion and fact are often very difficult to delineate.

### ***Anonymous Speech***

Online defamation presents added complications. Online, and in social media specifically, the source of the harmful communication is frequently anonymous. At the first line of attack, piercing the anonymity of the speaker can be challenging because of heightened standards under First Amendment and privacy laws. A plaintiff victim will often file his case against a Jane or John “Doe” defendant and seek to discover the identity of the defendant right after filing. The problem with this approach is that many courts require plaintiffs to meet heightened pleading and evidentiary standards before obtaining the identity of the defendant and, if plaintiffs cannot meet the heightened pleading standard to obtain the identity of the defendant, they will be unable to pursue their cases. In one leading case, a 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,” before 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.”<sup>99</sup>

### ***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 less exposure in operating these kinds of sites—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.<sup>100</sup> 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.<sup>101</sup> 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.

This early case law was superseded in 1996 by the CDA.<sup>102</sup> Section 230(c) of the CDA provides that: “[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.”<sup>103</sup> 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.”<sup>104</sup> 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 from claims arising from content posted to their website unless they participate in the creation or development of that content. Cases involving social media make the breadth of the immunity painfully clear. In *Doe v. MySpace, Inc.*,<sup>105</sup> 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.<sup>106</sup> The Texas District Court rejected the claim, and in doing so highlighted the potential breadth of the “immunity”:<sup>107</sup>

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 claims....

Recent case law has confirmed the CDA’s broad grant of immunity to republishers of interactive content. The Ninth and Tenth Circuits, for instance, recently affirmed the dismissal of actions against Google stemming from allegedly “discriminatory” search results and allegedly defamatory user reviews, respectively, based upon Google’s immunity from liability for third-party content under the CDA.<sup>108</sup>

Nevertheless, Plaintiffs continue to reach for creative attacks on Section 230. In *Finkel v. Facebook, Inc., et al.*,<sup>109</sup> the victim of alleged defamatory statements claimed

that Facebook’s ownership of the copyright in the postings barred its right to assert a Section 230 defense. 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.<sup>110</sup> 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.”<sup>111</sup> The *Finkle* decision is important because 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.

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.*,<sup>112</sup> the plaintiff argued that the operator’s immunity was defeated by the construction and operation of a 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.”<sup>113</sup>

In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,<sup>114</sup> the Ninth Circuit 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.<sup>115</sup> 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.<sup>116</sup>

The New York Court of Appeals, however, recently rejected a plaintiff’s contention that the CDA should not apply to a

real estate blog that allegedly “implicitly encouraged users to post negative comments.”<sup>117</sup> In fact, the Court held that “[c]reating an open forum for third parties to post content—including negative commentary—is at the core of what [the CDA] protects.”

Ultimately, 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.<sup>118</sup> 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.<sup>119</sup> Entities that operate social media sites therefore need to be especially careful not to allow their “editing” to turn into content creation or embellishment.

### **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.”<sup>120</sup> 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.<sup>121</sup>

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*,<sup>122</sup> 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.’”<sup>123</sup> 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.<sup>124</sup>

### **Reporter’s Privilege**

Application of existing rules to new technologies can raise yet more hurdles in speech cases. For example, suppose false or confidential information about your company appears on a blog. As part of damage control efforts, you may want to find the source of the information—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 have been 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.<sup>125</sup>

Although some courts have distinguished between the constitutional protections afforded to so-called “traditional” media and their non-traditional counterparts (e.g., bloggers),<sup>126</sup> the distinction has rapidly evaporated in recent years. In *Citizens United v. Fed. Election Comm’n*,<sup>127</sup> the Supreme Court noted that it has “consistently rejected the proposition that the institutional press has any constitutional privilege beyond that of other speakers” and further observed that, “[w]ith the advent of the Internet and the decline of print and broadcast media . . . the line between the media and others who wish to comment on political and social issues becomes far more blurred.” Most recently, in *Obsidian Fin. Group, LLC v. Cox*,<sup>128</sup> the Ninth Circuit, in the context of a defamation suit against a blogger, rejected the notion that “traditional” or “institutional” members of the press were entitled to a greater degree of protection under the First Amendment than their non-traditional counterparts: “The protections of

the First Amendment do not turn on whether the defendant was a trained journalist, formally affiliated with traditional news entities, engaged in conflict-of-interest disclosure, went beyond just assembling others' writings, or tried to get both sides of the story." The obvious import of this recent case law is that bloggers, in addition to the "traditional" press, are entitled to the "reporter's privilege" and need not disclose their confidential sources.

**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 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 the site operator itself rates products, services, or businesses, 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 post 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.*<sup>129</sup> In *Search King Inc. v. Google, Inc. v. Google Technology, Inc.*,<sup>130</sup> 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.'" 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."

Ratings sites that merely publish the reviews of third parties appear to enjoy broad immunity under the CDA. In *Levitt v. Yelp! Inc.*,<sup>131</sup> the plaintiffs in a class-action lawsuit alleged that Yelp extorted money from businesses that did not pay to advertise on its site by removing certain positive reviews, re-ordering reviews such that negative reviews appear at the top of the business listing, and even creating false negative reviews. The court dismissed plaintiffs' allegations, finding that plaintiffs had raised no more than a "possibility" that Yelp employees actually created negative reviews, and that the other two forms of alleged conduct – removing certain reviews and changing the order of appearance of certain reviews – "fall[] within the conduct immunized by [the CDA]."<sup>132</sup> Plaintiffs also argued that Yelp "creates" its aggregate business rating, which appears as a "star" rating at the top of each business's page, and that the aggregate content is therefore not shielded by the CDA. The court also rejected this theory, finding that the aggregate rating was "based on user-generated data" notwithstanding the fact that Yelp vetted its database to "filter out false reviews."<sup>133</sup>

Importantly, the court noted that Plaintiffs "in effect seek to import an intent-based exception into [the CDA], whereby the same conduct that would otherwise be immune under the statute... would no longer be immune when motivated by an improper reason, such as to pressure businesses to advertise."<sup>134</sup> Although "sympathetic to the ethical underpinning of Plaintiffs' argument," the court declined to give it effect, noting that the relevant section of the CDA contained no such exception, and that an intent-based exception would not only "prove problematic," but would also undermine the statutory purpose of "avoid[ing] the chilling effect of imposing liability" on providers of third-party content.<sup>135</sup>

**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.

### *Jurisdiction*

As a result of the greater protection given to reputation in comparison with other jurisdictions (such as the United States), the courts of England and Wales have in recent years become the forum of choice for some defamation claimants, regardless of whether there has been significant circulation in this jurisdiction. However, since the Defamation Act 2013 came into force on 1 January 2014, a new test will apply for actions against persons who are not domiciled in the UK, an EU member state or a Lugano Convention state. Under section 9 of the Defamation Act 2013, a court will not have jurisdiction unless it is satisfied that England and Wales is the most appropriate place in which to bring an action in respect of the statement. The court will have to look at the extent of publication globally to work out where it would be most appropriate for the claim to be heard.

### *What is defamation?*

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

- is defamatory (i.e. it tends to lower the claimant in the eyes of a right thinking person);
- identifies or refers to the claimant;
- is published by the defendant to a third party.

Under the Defamation Act 2013 there is a requirement for a claimant to show that the statement caused "serious harm" to its reputation in order for a statement to be defamatory. And a profit-making body must show that the statement has caused or is likely to cause "serious financial loss". The way in which the courts will interpret these provisions remains to be seen but it seems likely that it may make it more difficult than previously for companies to bring successful claims in defamation.

### *Internet-based defamation*

A number of claims have been made under English defamation law in respect of social networking sites. In October 2012 the New Zealand cricketer, Chris Cairns, successfully pursued a libel claim against Lalit Modi (a senior official in Indian cricketing) over Mr Modi's tweet alleging that Mr Cairns was guilty of match fixing. The tweet was originally published to only around 65 people. However, the Court of Appeal upheld an award of damages of £90,000 as it recognised that any comments could reach a wider audience very quickly, particularly when the original

audience was a specialist audience (here, a cricket loving audience).<sup>136</sup>

And many will be familiar with the case brought by Lord McAlpine against Sally Bercow (the wife of the Speaker of the House of Commons).<sup>137</sup> The proceedings followed a report which alleged that an unnamed conservative politician had been involved in the sexual abuse of boys in care. A number of tweets falsely linked him to the report, including one from Ms Bercow which stated "Why is Lord McAlpine trending? \*innocent face\*". It was held that Ms Bercow's tweet "joined the dots" and wrongly linked Lord McAlpine to the allegations, even though all she was doing was repeating information that was already online. The decision also illustrates how emoticons could be interpreted to demonstrate the meaning of a message to its readers.

### *Republication*

Until the introduction of the Defamation Act 2013 there was no single publication rule in English law. Previously a claimant had only one year from the date of publication to bring a claim for defamation but a fresh cause of action arose each time a statement was published (which meant that each hit on a website would constitute a fresh publication and the clock would start to run again). Under section 8 of the Defamation Act 2013 a cause of action will accrue on the first publication to the public or a section of the public and republication in "substantially the same form" as the first is not actionable. This will be helpful for those who hold archived content online.

### *Anonymous speech*

A Norwich Pharmacal order is an order which the English 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.

### *Internet service provider immunity*

A defendant must be the publisher of a defamatory statement in order to be liable for defamation. At common law the definition of a publisher is very wide and catches anyone who participates in the publication of a statement. That led to complaints being made against ISPs who were often seen as a easier target, as a poster might often be difficult to identify and not worth pursuing.

The Defamation Act 2013 provides that a person who was not the author, editor or publisher of a statement may not be sued for defamation unless the court is satisfied that it is not reasonably practicable to bring an action against a party who has actually published the statement. That is likely to offer protection to ISPs and hosts of social media content where it can be shown that they did not publish and did not have reason to believe that they were contributing to the publication of a defamatory statement.

It is likely that there will still continue to be some uncertainty as to whether an ISP (particularly one who exercises editorial control over statements) may be regarded as having published statements.

There is a defence pursuant to section 5 of the Defamation Act 2013 which is available to an operator of a website who did not post the statement and has acted without malice. However, the defence is defeated where a claimant can show that it was not possible to identify the person who posted the statement (which will be the case where the claimant has insufficient information to bring proceedings against them), the claimant gave the operator notice of the complaint about the statement and the operator failed to respond in accordance with provisions contained in regulations.

The Defamation (Operators of Websites) Regulations 2013 (the Regulations) which also came into effect on 1 January 2014 provide a procedure with which the operator of the website must have complied in order to benefit from the section 5 defence.

It is made clear in the new provisions that an operator of the website will not lose the defence by virtue only of having moderated the content of the website. However, exercising editorial control beyond mere "moderation" may well result in the website operator being unable to rely on this defence.

It seems likely that there will be litigation over who qualifies as an "operator of a website" and what is meant by "posting" a statement, as there are of course many ways in which a statement can find its way on to a particular site.

The new defence under section 5 is broader than those that remain available pursuant to regulation 19 of the E-

Commerce Regulations and under section 1 of the Defamation Act 1996. Regulation 19 only protects a party who has no 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 would lose immunity if, on obtaining knowledge of the illegal activity, it fails to act expeditiously to remove it or to suspend access to it.

Section 1 of the 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 or have reason to believe that what he did caused or contributed to the publication of a defamatory statement.

Section 5 will apply even where a website operator moderates content and/or becomes aware of the defamatory content by receiving a valid notice of complaint. However it will be important to comply with the procedure laid down by the Regulations, which could lead to a significant administrative burden depending on the number of complaints received by an operator.

The court has power under Section 13 of the Defamation Act 2013 to order a website operator (whether or not liable) to remove or to stop distributing a defamatory statement.

### *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 feed; 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 and other search engine sites causing for example a negative blog to be prominently listed when a customer types your organisation’s name into a 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 posters will time their communications to coincide with a key corporate event, such as the company’s earnings reports, in order to intensify the damage from the comment. The damage can be “done” in literally a matter of hours. A quick response can make all the difference. Accordingly it is important for companies to understand the risks to brand and reputation in social media, to have policies in place for managing internal and external communications, 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 the damage minimal.

Clients who find themselves on the end of a complaint should be prepared to act quickly in order to mitigate any damage done. And if the relevant websites are accessible in the UK, ISPs and other content hosts should be careful to follow the takedown procedure laid down by The Defamation (Operators of Websites) Regulations 2013 in order to benefit from the widest defence available. Content hosts should also require users to register before they are allowed to post so that they can be contacted if a notice of complaint is served. If the host has no email address, it must remove the post within 48 hours if it wants to rely on the Regulations to avoid liability. As a general point, it would be advisable to incorporate provisions in subscriber contracts giving the ISP or content host the right to remove material in certain circumstances (provided the right to remove is linked to reasonable and objective criteria).



## Chapter Authors

[Stephen Edwards](#), Partner – [sedwards@reedsmith.com](mailto:sedwards@reedsmith.com)

[Dr. Alexander R. Klett](#), Partner – [aklett@reedsmith.com](mailto: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<sup>138</sup>, 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<sup>139</sup> constant proactive monitoring of sites cannot be expected, an operator has an obligation to prevent subsequent evident infringements by the same infringer.<sup>140</sup> 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.<sup>141</sup> 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.<sup>142</sup> 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,<sup>143</sup> an original work in the UK sense<sup>144</sup>, or a personal intellectual creation as required under German copyright law.<sup>145</sup> 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<sup>146</sup> 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 may be needed, depending on which music is to be used. Some music is clearable through a single licence covering the whole of the EU, but 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 Authors<sup>147</sup>

### United States

[Kathleen A. O'Brien](mailto:kobrien@reedsmith.com), Partner – [kobrien@reedsmith.com](mailto:kobrien@reedsmith.com)

[Jennifer M. Westhoff](mailto:jwesthoff@reedsmith.com), Associate – [jwesthoff@reedsmith.com](mailto:jwesthoff@reedsmith.com)

## Introduction

This chapter explores key challenges which copyright owners face in the ever evolving world of social media.

In the last decade, the use of social media has exploded. For millions, social media is no longer a curiosity. Instead, it is now an integral part of their daily cultural, political, and social lives. As technology expands and becomes less expensive, more and more people have access to content online. Not only can they disseminate their own original content through social media, they can also access and use the content of others. This raises new challenges for copyright owners who seek to protect their valuable content from infringement and business owners who seek to use the content of others to promote their products and services through social media.

The following paragraphs discuss your rights with respect to copyrighted content under the following three common scenarios: (1) use of original content you have posted on a social media site by that site; (2) use of original content you have posted to a social media site by unauthorized third parties; and (2) your use of original content commenting on your business posted to a social media site by third parties. In each of these scenarios, your rights with respect to the dissemination of the content differ.

### Use of Original Content You Have Posted on a Social Media Site by That Site

The terms of service for many social media sites like Twitter<sup>148</sup>, Facebook<sup>149</sup>, Instagram<sup>150</sup>, and YouTube<sup>151</sup> give the site a non-exclusive royalty-free license to use the content you post. On some sites, such as Pinterest, that license is limited to use on just that site. But on other sites, such as Facebook, and by extension Instagram<sup>152</sup>, by posting any content to your wall, you grant the site broad rights to use that content, including in advertising which appears on the site. For this reason, it is important to read and understand the scope of any license you are granting to a social media site before posting content there.

### Use of Original Content You Have Posted on a Social Media Site by Unauthorized Third Parties

Although you may understand and view a social media site's use of your content as a quid pro quo for your use of that site, do you have a different view if another user, or another website, accesses your copyrighted content and reposts it for their own purposes? In 2010, a photojournalist named Daniel Morel was in Haiti when the earthquake struck. Morel took a now iconic photograph of a woman peering out of the rubble and posted it to Twitter using a third-party service called TwitPic. The next day, Agence France Presse (AFP) and Getty Images picked up the image and began publishing it with stories about the earthquake. Morel, who had not authorized the use of his photograph, sent cease-and-desist letters to both

companies. AFP responded with a lawsuit claiming “antagonistic assertion of rights.”<sup>153</sup> AFP claimed that Twitter’s terms of service gave AFP a non-exclusive license to use, copy and distribute the photograph. In January of 2013, US District Court Judge Allison Nathan found that AFP’s unauthorized use of the photograph in various news stories violated Morel’s copyright. In November of that same year, a jury found that AFP’s infringement was willful and awarded Morel \$1.2 million, the highest statutory damages available.<sup>154</sup> The *Morel* case suggests that although individual social media sites may use a user’s content for site purposes, third parties may not mine social media sites for free content. Unfortunately, at this juncture, the case law on point is very limited and many questions remain unanswered.

The anonymity of the Internet emboldens users to engage in conduct that they would never consider otherwise. When a writer misappropriates a copyrighted work in print or film, the media backlash can be immediate. But when a user misappropriates a work on the Internet where pseudo-names and IP addresses can change faster than the latest Hollywood fashions, how can you protect yourself? If a third party is using your copyrighted content without your permission on a major social media site, such as Facebook, Twitter, or YouTube, whether it is edited without your consent or posted without proper credit, the quickest recourse is to seek to have the item removed by sending a takedown notice under the Digital Millennium Copyright Act (DMCA) to the user and the owner of the social media site. The DMCA protects copyrighted works by prohibiting unauthorized digital duplication through the criminalization of technology, devices, or services intended to circumvent the measures meant to control access to the copyrighted works.<sup>155</sup> To facilitate online service provider (OSP)<sup>156</sup> compliance with the DMCA, all OSPs are required to implement a notice and take down procedure that allows copyright holders to notify the OSP that it is hosting infringing content.<sup>157</sup> If you find an infringing copy of your work on a social media site, you can fill out a notice form or send an email notice to a designated contact person at that site which contains the following: (1) your name and contact information; (2) information that identifies the allegedly infringing work; (3) information that identifies the work that you are claiming has been infringed; (4) a statement that the you have a good faith belief that infringement has occurred; (5) a statement that you are authorized to act on behalf of the copyright owner; and (6) a statement that the information in the notification is accurate.<sup>158</sup> When large, well-established social media sites like Facebook<sup>159</sup>, Twitter<sup>160</sup>, or YouTube<sup>161</sup> receive notice of a potential copyright infringement, they will first take down the allegedly infringing content and then alert

the poster of that content of the infringement claim. The poster can either do nothing, in which case the content will no longer appear on the site, or send a counter-notice to the social media site which disputes your copyright infringement claim, in which case the site will notify you that the poster disputes your claim. If you fail to file a lawsuit within 10-14 business days of your receipt of the counter-notice, the social media site can put the work back up<sup>162</sup>.

Even if the infringing content is removed, there may be circumstances in which litigation is the only means available avenue to obtain the relief you seek, for example, in circumstances in which you have suffered serious economic injury or the infringer posts the infringing content on a multitude of websites at a rate that would require you to hire a small army to keep up with the necessary take down notices and you need to obtain an injunction to stop that conduct. One benefit to a counter-notice is that the accused infringer must identify himself by providing his true name and bona fide contact information. This provides you with an actionable defendant should you decide to pursue litigation. However, if the accused infringer fails to file a counter-notice, determining his true identity may prove to be a real challenge. Unfortunately, a social media site’s obligation to assist you often begins and ends with the DMCA notice and take down procedures. If the infringer fails to file a counter-notice, it is likely to take either a subpoena or a court order to compel the social media site to hand over his contact information and aside from his IP address, they may not have bona fide identification information to provide to you. A number of courts have found that an IP address is not enough to satisfy the court’s pleading standards for an actionable defendant. For example, in *Elf Man, LLC v. Cariveau*, in January of 2014, a federal judge in Washington State, relying on the landmark opinions in *Perfect 10 v. Amazon.com, Inc.*<sup>163</sup>, *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*<sup>164</sup>, and *Ashcroft v. Iqba*,<sup>165</sup> held that an IP address linked to an individual defendant was not sufficient or specific enough evidence to create an actionable claim against that defendant.<sup>166</sup> In that case, the judge gave the plaintiffs more time to gather more specific evidence linking the IP address owner to the infringement but also voiced his sincere doubt that such evidence could be found.<sup>167</sup> The problem is that an IP address, particularly one which is linked to an internet café, public library or some other public site, does not place a specific individual in the chair in front of the computer at the time your copyrighted work was posted. Under these circumstances, having enough evidence to (1) bring suit against the infringer; and (2) actually prove infringement can be a daunting task. In a

world where the only trace of an infringer is his IP address, you may have little viable recourse against him.

## Your Use of User Generated Content

One of the benefits of social media is that it gives you the ability to collect information about how your customers perceive your business and the goods or services that you offer. Social media empowers consumers to heap praise or air grievances and many businesses can trace success or failure back to their online reviews. But who owns those reviews? If a Yelp user reviews your restaurant positively, can you use their glowing remarks in advertising? If a client Tweets about the excellent service they received at your hair salon, can you post that to your Facebook page? Generally, the review is owned by the author who posts it and your ability to use it is governed by the terms of use of the social media site on which the post appears. While you always should pay close attention to the terms of service of the specific social media site at issue, there are some general guidelines that you can follow when you seek to use such user-generated content (UGC).

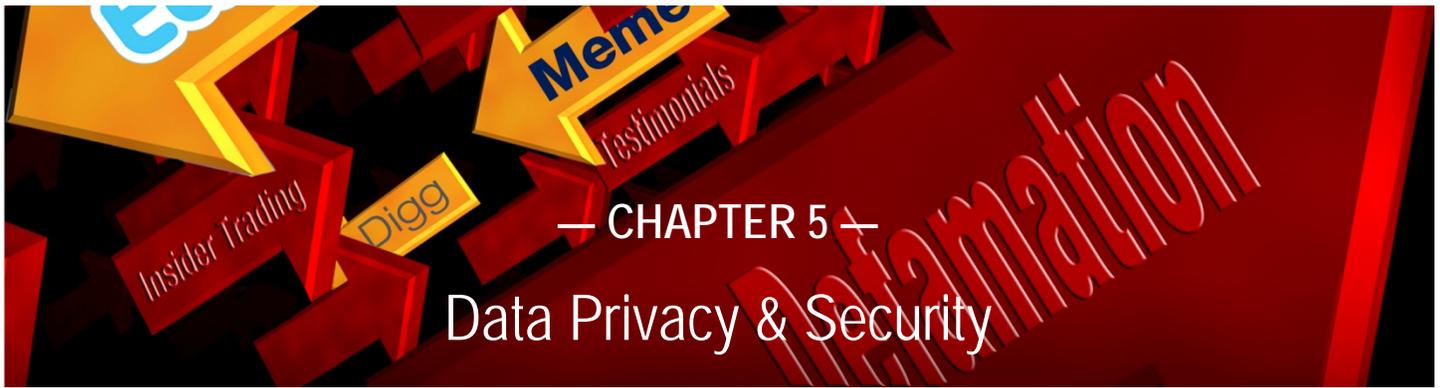
Typically, companies seek to use UGC either through republication on the same social media site, such as a retweet, or through publication of the comment in a different way, either in print or at a different online location. Generally, the reposting of UGC in the same forum in which it was originally posted, such as retweeting a tweet or highlighting a Facebook comment, is a lawful practice which falls within the terms of service to which the original poster agrees. In contrast, issues arise when a company seeks to post UGC in a new location, whether it's a screen shot posted to the company's website or a review republished in print advertising. In most cases, the site's terms of service recognize that the author is the owner of the content. As a result, you should ask the author's permission of the author before republishing his UGC elsewhere. It is important to understand that different websites have different policies even if you obtain the author's permission to use his UGC. For instance, Facebook prohibits the use of UGC in advertisements even if the author grants permission,<sup>168</sup> while Twitter will allow

such use in most cases as long as the author has granted permission.<sup>169</sup>

The safest way to obtain UGC that can be used in advertising is to directly solicit such content from users. Any solicitation should be accompanied by a set of rules for submitting content which protect third party rights. Typical rules prohibit the submission of content which is not the original work of the submitting party, including content which (1) is the subject of any copyright or trademark owned by a third party; (2) contains the name, image or likeness of any third party; or (3) is defamatory. Additionally, your business must follow the Federal Trade Commission's Guides Concerning the Use of Endorsements and Testimonials in Advertising,<sup>170</sup> as well as all state laws and guidelines.

## Looking at the Future: Social Media and Your Copyrights

Social media is no longer the business of plucky Harvard undergrads and creative friends. It is a billion dollar industry in which profits are generated by engaging users and inundating them with ads and the opportunity to make purchases. The business of social media has become adept at monetizing its users. Twitter and Facebook are now publicly traded -companies; Facebook and Google have made billion dollar purchases of other social media sites. So what does this mean for your business? You now must be more vigilant than ever to protect your original content. If your company uses InstaGram, that content is now subject to Facebook's terms of service. If your company posts on YouTube, your content is now at the mercy of Google. Social media sites can change their terms of service at their whim and can claim license or ownership over your content. Every copyright holder who uses social media must remember that it is a business whose goals may be at odds with your own. As the business of social media continues to evolve rapidly so must your company's strategy to both take advantage of its benefits and safeguard your own rights.



## Chapter Authors<sup>171</sup>

### United States

[Paul Bond](#), Partner – [pbond@reedsmith.com](mailto:pbond@reedsmith.com)

[Mark S. Melodia](#), Partner – [mmelodia@reedsmith.com](mailto:mmelodia@reedsmith.com)

[Christine Nielsen Czuprynski](#), Associate – [mcczuprynski@reedsmith.com](mailto:mcczuprynski@reedsmith.com)

[Lisa Kim](#), Associate – [mlkim@reedsmith.com](mailto:mlkim@reedsmith.com)

[Frederick Lah](#), Associate – [mflah@reedsmith.com](mailto:mflah@reedsmith.com)

### United Kingdom

[Cynthia O'Donoghue](#), Partner – [codonoghue@reedsmith.com](mailto:codonoghue@reedsmith.com)

## Introduction

According to statistics published on Facebook,<sup>172</sup> over a billion people use Facebook monthly. That's one out of every seven people in the world. Nowadays, most major brands have a presence on at least one of the main social media platforms, whether it be Facebook, Twitter, Pinterest, Tumblr, Instagram, or Foursquare. The social media market is constantly expanding too, with newer social media offerings like Vine, Snapchat, and Jelly popping up and gaining popularity.

The benefits of social media are clear -- social media helps companies stay connected and interact with their customers about new promotions, offerings and products. On the other hand, social media poses unique risks, particularly with respect to data privacy. The effects of a data breach for a social media company can be particularly harmful because of the high number of users. And as social media companies continue to find new, innovative ways to collect, use, and monetise their data, they will continue to be scrutinized by regulators and serve as an attractive target to class action lawyers. Since the publication of our last version of this White Paper, both the Federal Trade Commission ("FTC") and the United States Department of Commerce have developed guidance to help companies in their efforts to protect the privacy of consumers and Internet users.<sup>173</sup> In addition, there have been other amendments to federal and state laws to account for new technologies. There have been developments from an international aspect as well.

## Social Media in Action in Data Privacy & Security

Personal data collected by social media companies is at risk from all sides. Thieves and hackers want to steal and resell personal 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.<sup>174</sup> Even standard business processes pose risks to personal data. Social media enterprises collect, store, use, share, and dispose of personal data every day, including 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.

And let's not forget the value that this information possesses. In this age of Big Data, virtually all companies, not just social media companies, are looking to utilize and gain commercial leverage from the data collected. It should come then as no surprise that regulators and plaintiffs' lawyers are focusing their efforts not just on data breaches, but also on data practices. Over the past few years, various regulatory investigations and class action lawsuits have been brought against social media companies over their alleged collection, use, and sharing practices, and the choices consumers have with respect to those practices. This chapter explains some things social media companies and companies that use social media should know in this ever-evolving space.

### *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, in both the US and Europe, best practice is to separate the privacy policy from the terms of use. In addition, websites targeting persons in the European Economic Area<sup>175</sup> and Mexico need to include information on the types of storage or cookie technologies used and the purpose. Users must consent to the placement of cookies on all devices, computers, tablets, mobile phones, etc., and be given the opportunity to opt out of having those items placed on their devices. Where cookies are used, individual must be provided with clear and transparent notice about cookie use. Creating a separate document, page or display makes these terms conspicuous and creates better "notice and disclosure" or transparency for consumers.

Cookie policies are statements about what types of cookies may be set by a website and for what purposes they may be used and should also give users information on how to either opt out or change their browser settings. 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.<sup>176</sup> 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 cookie policies and 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, namely terms of use and privacy policy agreements.<sup>177</sup> The increase in focus on such user agreements has resulted in regulatory and consumer scrutiny for some social media companies, most notably Facebook and its one billion users.

Nearly every change Facebook has made to its privacy policy over the past few years has drawn a lot of attention. In December 2009, Facebook made changes to its privacy policy that caught the eye of the Federal Trade Commission and ultimately lead to a settlement, which was announced in 2011.<sup>178</sup> The FTC's complaints centered mostly on Facebook's alleged misrepresentations in its privacy policy, which it had unilaterally implemented without notice to its users.<sup>179</sup> Specifically, the FTC alleged that Facebook shared information with advertisers when it promised not to, and though it promised to verify the security of what it called "Verified Apps," it did not in fact do so. The FTC, after an open comment period, approved the settlement in August 2012.<sup>180</sup> In November 2012, Facebook again announced changes to its privacy policy, which drew the concern of privacy advocacy groups.<sup>181</sup> In

August 2013, Facebook proposed clarifications to its privacy policy, this time centered around the use of profile information for advertising purposes. Following complaints from privacy advocates that the changes may be contrary to Facebook's 2011 settlement with the FTC, the FTC stated that it was monitoring whether the changes complied with that settlement.<sup>182</sup> In November 2013, Facebook affirmed the changes in a blog post that explained how and when profile information was used in advertising.<sup>183</sup> In October 2013, Facebook made another privacy change, this time affecting teenagers. Facebook users age 13-17 had previously not been able to change their privacy settings to allow for the general public, rather than just their "friends," to view their posts, but that rule was relaxed.<sup>184</sup>

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 and the European Union Lisbon Treaty explicitly provides that data protection is a fundamental human right. There is also a greater focus on raising awareness. For example, Europe even organised a "European data protection day", held annually on 28 January.<sup>185</sup> 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.

Google, for example, has had its fair share of scrutiny. The European Court of Justice (ECJ) has been embroiled in numerous disputes involving Google. In 2010 Louis Vuitton brought a case against Google France for trademark infringement for the supply of their luxury trademark to advertisers as keywords as part of Google Adwords.<sup>186</sup> In this case the ECJ found in favour of Google, declaring that brand owners will not be able to stop Google from selling their trademarks as keywords to competitors to trigger advertisements through Google Adwords, provided the advertiser clearly shows they are not the trademark proprietor.<sup>187</sup> The ECJ also mediated in a case against Google Inc. and Google Spain S.L referred by Spain's highest court the Audiencia Nacional de España. This case tested the principle of the 'right to be forgotten' in the EU whereby individuals demanded the deletion of their data from the data host's search engine results.<sup>188</sup> The ECJ declared Google could not be considered a controller of personal data appearing on web pages which it processes and also found in Google's favour ruling that an internet search engine provider cannot be required to withdraw information from its index. In the interests of freedom of

expression the ECJ held a subjective preference does not amount to a compelling legitimate ground for a person to restrict or terminate dissemination of their personal data on internet search engines, even where harmful or contrary to their interests.<sup>189</sup>

More recently in 2014, a high court in the UK has announced<sup>190</sup> that Google must face a breach of privacy claim brought by a group of over 100 claimants known as the 'Safari Users Against Google's Secret Tracking.'<sup>191</sup> The group claims that Google misused their private information, bypassing their privacy settings to unlawfully monitor their browsing history by placing secret cookies on Apple Inc.'s Safari browser.

Google has also found itself in hot water with data protection authorities across Europe following changes to its privacy policy in March 2012 which triggered investigations in Germany, Italy, UK, Italy, Netherlands, Spain and France<sup>192</sup> as well as in South Korea.<sup>193</sup> Google's changes to its privacy policy resulted in it consolidating its 60 privacy policies into one document, which controversially permits Google, without consent, to combine data collected from users across all Google services including Google Search, Google Chrome, Gmail, Google DoubleClick advertising, Google analytics, Google maps and You Tube. The privacy policy GPP2012 has been found to be incompatible with EU and other countries' data protection laws for failing to provide users with sufficient information about how their browsing data is collected and used, or giving them an opt-out. Critics have called for the policy changes to be reversed;<sup>194</sup> however, Google has failed to take any action to date. As a result Google is now facing fines of €150,000 in France<sup>195</sup> and €900,000 in Spain.<sup>196</sup> Critics have condemned the fines as an insufficient deterrent, just pocket money for Google. However imminent reform in EU data protection law could mean Google will be forced to pay attention, given that the level of possible sanctions proposed under the draft Data Protection Regulation could result in a fine of up to or 5% of worldwide annual turnover.<sup>197</sup>

Facebook has not escaped the headlines, especially when in December 2009 it struggled to get the balance right when it changed its site by making user's profiles publicly accessible by default, in turn prompting many users to switch social networks.<sup>198</sup> Facebook was also publicly criticized following a subject access request by an Austrian student which exposed that Facebook retains personal data about users infinitely, even after users had the information from their account.<sup>199</sup> Lobbying by the student group Facebook v. Europe<sup>200</sup> prompted the Irish Data Protection Commissioner to conduct an audit of

Facebook's data processing practices in 2011.<sup>201</sup> Facebook largely complied with the audit reports recommendations, including for example, by simplifying its privacy policy, adding a tool that allows users to see all data held about them, changing to the 'like' button to remove the last octet of logged IP addresses, and suspending its facial-recognition tool. In 2011, however, the German data protection authority further challenged the legitimacy of Facebook's facial recognition feature on the basis that it required users to actively opt-out if they did not want their details to be collected and referenced for tagging purposes.<sup>202</sup> In 2012 the German data protection authority also issued a decree demanding that Facebook change its controversial real name policy to allow users to adopt pseudonyms in the interests of privacy.<sup>203</sup>

#### *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. As discussed below, most of the major social media networks offer page administration options for content removal on company-sponsored portals though, there are variations as to how each of those options work. In general, though, the company can directly control content posted to the portal by designating in its administrative options to pre- or post-screen user-generated content.

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.<sup>204</sup> Alternatively, companies could issue cease-and-desist e-mails directly to the employee posting the content on YouTube.
- **On Twitter the answer is probably no, also.** The Twitter Rules prohibit posting "other people's private and confidential information, such as credit card numbers, street address or Social Security/National Identity numbers, without their express authorization and permission."<sup>205</sup> The remedy for removing that content is to report the violation of the Rules, but the report can only come from the person to whom the private information belongs.<sup>206</sup>
- **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").<sup>207</sup> In Section 5 of the Terms, Facebook will not permit posting of "anyone's identification documents or sensitive financial information on Facebook."<sup>208</sup> 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 Instagram the answer is possibly.** On Instagram, the remedy for removing content is reporting an abuse of Instagram's Community Guidelines.<sup>209</sup> Those Community Guidelines have a general prohibition against "being rude," which can involve using the service to "abuse, attack, harass or impersonate others."<sup>210</sup> If the company could make a case that the post was made to abuse and attack, Instagram might be persuaded to remove the video.
- **The same is true for Pinterest.** The Pinterest Acceptable Use Policy prohibits posting any content that "may create a risk of any other loss or damage to any person or property" and that "contains any information or content that the poster do not have a right to make available under any law or under contractual or fiduciary relationships."<sup>211</sup> Pinterest reserves the right to remove any content that violates the Terms of Use or the Acceptable Use Policy<sup>212</sup>, and allows others to report violations of those policies.<sup>213</sup> If Pinterest believes the content violates its policies, it will remove the offending content.

- **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.<sup>214</sup> Under the Terms of Use Agreement in Section 8, any postings that would violate the privacy rights, publicity rights, and/or any other rights of any person are prohibited.<sup>215</sup> 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. Snapchat, a photo sharing app, allows users to edit and share photos with their friends and to set a time limit for how long the recipient can view the photos. After the photos are viewed, the photo is then deleted from the device and Snapchat's servers. After a forensic researcher claimed that the images sent via Snapchat are recoverable and do not in fact disappear forever,<sup>216</sup> the company experienced negative backlash from the press and its users. In response, Snapchat released a public statement describing in detail how the images are stored and deleted, reassuring users that the images are deleted from its servers and user devices after viewing. Snapchat did note, though, that it is possible to access the files by circumventing the app and "jailbreaking" the phone with the right forensic tools.<sup>217</sup>

Further concerns may arise from users about how their data is utilized by social networking sites. Social media companies employ technological measures that recognise a user's computer, and in some cases, the companies may use the same technological measures to participate in a behavioral advertising network or assist in the collection of data for analytics. In a push for more transparency in the collection of this data, the FTC Privacy Report advocates for "Do Not Track," a mechanism meant to give the user more control over the collection of the data that identifies his or her computer. While Do Not Track is by no means a legal requirement, even if the user selects the feature in his or her browser, some companies have publicly supported the feature, such as Twitter<sup>218</sup> and Pinterest.<sup>219</sup>

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 what qualifies as adequate protection than its counterparts in the European Union and other parts of the world. A social media company's practices can be compliant with United States law and still run afoul of legal mores elsewhere. By way of example, in January 2013, WhatsApp, the instant messaging and media sharing mobile app, was said to have violated Canadian and Dutch privacy laws in a report published by those countries data protection authorities. The report said that the app had violated privacy laws because users were not given the choice as to whose contact details they had to share with WhatsApp and that users were forced to provide their entire address book – both users and non-users.<sup>220</sup> While the FTC did not bring an action against WhatsApp for these alleged privacy violations, they did end up entering into a consent decree with Path, a social networking journal service, over similar charges. In the complaint, the FTC alleged that the user interface in Path's app was misleading and provided consumers with no meaningful choice regarding the collection of their personal information. The FTC alleged that Path automatically collected and stored personal information, such as name, address, phone numbers, email, Facebook and Twitter usernames, from the user's mobile device address book even if the user had selected the "Find friends from your contacts" option.<sup>221</sup>

### *Europe position*

Social media services accessible in Europe will also have to comply with the relevant Data Protection Directive 95/46/EC, the implementation of which differs between the 28 EU Member States, and they may also be subject to any additional national measures. At present the existing Directive is set to be overhauled and may be replaced by a more coherent and comprehensive legislative package: a General Data Protection Regulation<sup>222</sup> and a Directive.<sup>223</sup> Drafts were first published in January 2012 and there were high hopes for a swift reform, however, the controversial

substantive content of the proposals has resulted in protracted debate.<sup>224</sup> As a result, recent comments from the European Commission indicate that the legislative package may not be adopted until 2015 at the earliest.

Specific elements of the proposed Regulation could significantly impact social media companies, Article 20 will provide individuals with the right to object to a social media company profiling them on the basis of their social media account content. The right of data portability under Article 18 will also make it easier for individuals to switch social media service providers, taking with them a copy of all their account data in electronic format. Social media sites also face onerous obligations in relation to Article 17 which expands the 'right of erasure' under the Directive 95/46/EC which would allow users to request the deletion of all objectionable data replicated on third party hosting web pages such as links and posts on social media sites. The potential burden of this obligation was highlighted in a recent court case in the High Court of Ireland<sup>225</sup> where a student was wrongly accused of a crime in a Facebook post that went viral. The court held the distress caused to the individual justified 'the right of be forgotten'. As a result, a mandatory injunction was granted, ordering YouTube, Google and Facebook to take down the offending material about the individual within 14 days. This judgment alone could set a precedent for further cases involving individuals objecting to offending material about them on social media sites and has the potential to conflict with the right to freedom of expression.

The EU's Article 29 Data Protection Working Party has set forth an opinion on online social networking.<sup>226</sup> 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."<sup>227</sup> 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.<sup>228</sup> 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.<sup>229</sup>

The ICO published guidance in 2013 on how the Act applies within the context of social networking and online forums.<sup>230</sup> An exemption from the Act applies in limited circumstances to individuals who process personal data for domestic purposes only. Where this exemption does not apply, any individuals uploading personal data on online forums and social media sites, and organisations running those sites, are deemed data controllers under the Act and must adhere to certain responsibilities. This includes taking reasonable steps to check the accuracy of any personal data posted on sites by third parties. To satisfy this obligation, the ICO recommends having a clear and prominent policy about acceptable and non-acceptable posts, as well as implementing a complaints mechanism to deal with any disputes concerning inaccurate posts and a procedure to delete such posts.

### *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. Recent regulatory guidance from the ICO<sup>231</sup> supports the use of transparent, clear and simple privacy policies which adapt a "layered" approach, with the most important information highlighted in a clear manner. The ICO requires organisations to take proactive steps to visibly communicate a privacy policy, preferably via the same method through data is collected. 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.<sup>232</sup>

Privacy policies should be reviewed regularly to make sure that they continue to comply with any changes in the data processing activities of a social media company and the relevant data protection and privacy laws applicable. If not, they can expose a company to possible regulatory enforcement. Over the past few years, both Facebook<sup>233</sup> and Myspace<sup>234</sup> have been hit with deceptive charges by

the FTC over their allegedly misleading disclosures in their privacy policies. In both cases, the FTC alleged that the companies' information sharing practices were inconsistent with the promises set forth in their privacy policies.

Aside from the social media companies themselves, companies who simply offer users the ability to share or "Like" content from their own pages should also make the appropriate disclosures in their privacy policies as to the type of information they share and access from social media platforms.

In addition to avoiding regulatory scrutiny, there are other 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 235*

Privacy and data protection law will continually be outpaced by technological developments. As such, the main challenge for social media companies is that the privacy "obligations" seem to be developing on-the-fly in this area. For example, in 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. Facebook even provided a pop-up, opt-out mechanism to help respect subscriber privacy choices. Despite the fact that there were no US laws clearly prohibiting this practice, soon after Beacon's launch, a civic action group created a Facebook group and online petition demanding that Facebook not publish their activity from other websites without explicit permission from the user. In less than ten days, this group gained 50,000 members. Beacon amended its Terms of Service as a result. A class action lawsuit was filed against Facebook as a result of Beacon. The lawsuit was ultimately settled in September 2009, and the Beacon advertisement service was shut down. Facebook also agreed to donate \$9.5 million to a non-profit foundation to promote online safety and security.<sup>236</sup>

More recently, Facebook fought off litigation in connection with its Sponsored Stories advertising campaign, where Facebook delivered users ads featuring the photos and names of friends that had "liked" the companies sending the ads. In that case, Facebook faced allegations that it

had failed to adequately disclose to users the extent to which their likeness and names would be used in advertisements, and thus, allegedly failed to garner consent as required by California law.<sup>237</sup> That case eventually settled, with the judge approving a \$20 million settlement.<sup>238</sup> In addition, Facebook announced that it would be dropping its Sponsored Stories campaign.

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, without, at a minimum, adequate disclosures. 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.

Leading industry groups have stepped up to assist in this area by developing self-regulatory principles to guide companies in this area. The "Self-Regulatory Principles for Online Behavioral Advertising,"<sup>239</sup> which were created and released in 2009 as a joint business initiative by the American Association of Advertising Agencies, Association of National Advertisers, Interactive Advertising Bureau, Direct Marketing Association and the Better Business Bureau, identifies seven principles to guide companies in this advertising space. The principles, which correspond with self-regulatory principles proposed by the FTC, are: education, transparency, consumer control, data security, material changes, sensitive data and accountability.

These Principles are more than just guidelines. The Council of Better Business Bureaus, along with the trade groups, created a corresponding Interest-Based Advertising Accountability Program to review the practices of companies in the online advertising space and foster the widespread adoption of them. To date, the Accountability Program has issued more than 20 decisions identifying instances of non-compliance.<sup>240</sup>

This initiative appears to have now crossed over to Europe. The Article 29 Working Party has published several opinions<sup>241</sup> on online behavioural advertising including best practices to comply with the E-Privacy Directive<sup>242</sup>, which requires an organisation to obtain a user's prior informed consent to collect cookies for the purposes of

targeting online behavioural advertising. The Article 29 Working Party has also publicly supported industry initiatives to establish a European wide self-regulatory standard. For example the European Advertising Standards Alliance (EASA) and the Internet Advertising Europe have adopted a ‘Best Practice Code For Online Behavioural Advertising.’<sup>243</sup> The European Interactive Digital Advertising Alliance<sup>244</sup> has also launched an interactive icon to be displayed on advertisements, to provide users with information about how and why a particular advert was targeted and delivered to them, including the opportunity to opt-out.

In the UK the Committee of Advertising Practise (CAP), which writes and maintains the UK advertising codes, specifically introduced rules for organisations conducting online behavioural advertising.<sup>245</sup> These rules require organisations to provide users with a comprehensive notice about what web viewing behaviour is being observed and that the organisations seek explicit consent to use such data for the purposes of online behavioural advertising.

Another social media phenomenon is the exploitation of geo-location technology. Many social media networks, such as Foursquare, have incorporated “check-in” functions whereby the user can disclose their arrival to a particular physical place. By “checking-in,” the user opens themselves up to location-based advertisements, such as recommendations of places to go, things to do nearby, and tips from other users for that location, as well as advertises for that particular “check-in” location. For example, Yelp, an “online urban guide” and business review site encourages businesses to offer “Yelp Check-in Offers” so that customers are incentivized to broadcast to their friends that they are at the business’ location.<sup>246</sup> Although these features clearly have some benefit to the user, the collection of geo-location information, especially when not necessary to the functioning of the mobile application or adequately disclosed to the user, has caught the attention of regulators and attorneys generals alike.

In February 2013, the FTC issued a staff report recommending ways in which critical players in the mobile market can better inform consumers about their data practices. These recommendations particularly addressed the collection of sensitive content, like geo-location information, and recommended, among other things, that there be just-in time disclosures to consumers to obtain their affirmative express consent before allowing collection of such information.<sup>247</sup> Similarly, the CA attorney general Kamala D. Harris—one of the most active attorney generals in the privacy space—also issued her own recommendations to assist those in the mobile

marketplace, which emphasized only collection information and data necessary for an app’s functionality and special notices to draw attention to data practices that may be unexpected.<sup>248</sup> Regulatory actions addressing these mobile privacy concerns have already begun.<sup>249</sup>

### *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.

- Monitoring of individuals on social media sites is increasingly controversial in the context of Edwards Snowden’s revelations about mass surveillance activities in America by the NSA.<sup>250</sup> This has triggered the exposure of further mass surveillance within the EU by the governments of certain Member States. This has called into question all transfers of data operating under Safe Harbor certification and could result in Europe shutting boundaries to all cross-border transfers of data.<sup>251</sup>
- Employer-employee relationships are being increasingly tested, by disputes concerning social media accounts operated by employees on behalf of their employers. For example in the UK courts have debated whether employees or employers are deemed to own any client contact information generated by employees on behalf of their employers via LinkedIn.<sup>252</sup>
- Social media sites are routinely used for sting operations seeking out sexual predators and other criminals.<sup>253</sup>
- A New York court admitted evidence from the plaintiff’s Facebook page offered to disprove claims that the plaintiff’s injuries resulted in a loss of enjoyment in life reasoning that a user of social media does not have a reasonable expectation of privacy in information shared with others through Facebook, notwithstanding her privacy settings.<sup>254</sup>
- The alteration or destruction of posts on social media sites can lead to sanctions for spoliation.<sup>255</sup>
- A Canadian court allowed discovery of a Facebook profile in a motor vehicle accident suit, despite the document being subscriber-designated as limited access.<sup>256</sup>
- An Oklahoma court has evaluated whether invitations to Twitter and Facebook posts were considered

violations of an former employee's non-solicitation agreement.<sup>257</sup>

- Employees' social media posts have formed the basis for wrongful discharge claims.<sup>258</sup>
- 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.<sup>259</sup>
- Subscribers' posts may violate their own company's privacy policies, or even reveal their own company's trade secrets.<sup>260</sup>
- Libelous posts on social media sites have been found to be actionable.<sup>261</sup>
- Recent court rulings have highlighted that traditional methods of service are being abandoned in the favour of substituted service via social media.<sup>262</sup> A landmark decision in Australia<sup>263</sup> and a similar ruling in New Zealand<sup>264</sup> first permitted service by Facebook where the defendants' whereabouts were unknown save for their profile on a social media site. Another court case in Canada<sup>265</sup> ruled it was permissible to notify a defendant of court proceedings by sending a message to their social media account inbox. Following the trend, a High Court Judge in the UK allowed an injunction to be served on a defendant through Twitter for the first time<sup>266</sup> setting the precedent for a High Court ruling permitting service via Facebook in 2012.<sup>267</sup> Evidently courts are increasingly prepared to deploy modern technology in support of litigants needing to serve unscrupulous opponents. Service by social media is now becoming the routine norm, rather than the exception in today's technological society where our presence online is increasingly visible.

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 potentially risky behaviors. In January 2013, the FTC adopted amendments to COPPA to account for evolving technologies and the ways in which children are accessing the Internet through mobile devices and social networking. The final amendments include expanding the scope of "personal information" to include geolocation information if precise enough to identify a name of a street and city, photographs or videos containing a child's image, a screen or user name to the extent that it functions as online contact information, and persistent identifiers if it can recognize a user over time and across different websites. Social media companies may end up collecting one or all of these pieces of data in the course of their everyday operations. To the extent that they are collecting this data from children under 13 years of age, they will need to comply with the requirements of COPPA.<sup>268</sup>

Children's privacy has become a state issue as well recently, with California having passed an "eraser button" law, the first of its kind in the U.S. The law, which takes effect January 1, 2015, applies to operators of websites and mobile apps, such as social media companies, whose products and services are directed toward minors (defined as under age 18), and who have actual knowledge that their products and services are being used by minors. Under the law, these operators will be required to notify minors of their right to remove posted content and provide instructions on how to do so.

The impact of digital media on privacy issues for young people has been a key focus in both the UK and throughout Europe. A central theme of the 35th International Conference of Data Protection and Privacy Commissioners<sup>269</sup> was the 'application of society' with children's privacy rights becoming increasingly vulnerable as young people become more addicted and dependent on the internet and social networking.

A central aim of the European Digital Agenda is to address the dilemma that growing numbers of children are on social networking sites but do are not taking the necessary steps to protect themselves, failing to set their profile settings to private, and therefore placing themselves in harm's way. Recent surveys conducted highlight that 77%

of 13-16 year olds and 38% of 9-12 year old in the EU have a profile on a social networking site, with 25% setting their display settings to 'public'.<sup>270</sup> A recent CNIL, the French data protection authority, study by the Department of Studies, Innovation and Foresight as part of their reports for "Privacy 2020" also found children to be the most active user group for photo sharing and tagging on social network sites.<sup>271</sup>

To achieve a safer internet environment for children, the European Commission and major social networking companies, including Facebook, Bebo, and MySpace, agreed the "*Safer Social Networking Principles for the EU*".<sup>272</sup> 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<sup>273</sup>; empowering users through tools and technology to manage the service<sup>274</sup>; 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.<sup>275</sup> 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.

In 2011 the European Commission supported a further initiative, the CEO Coalition To Make the Internet A Better Place For Kids.<sup>276</sup> Most recently, the European Commission announced the launch of 'Safer Internet Day' on 11 February 2014 where Vice President and Commissioner of the Digital Agenda Neelie Kroes, will grant European Awards for websites with Best Online Content for Kids.<sup>277</sup>

In the UK, the Information Commissioner has published numerous good practice notes for website operators whose sites are directed at children including the "Personal Information Online Code of Practice."<sup>278</sup> The Home Office Task Force on Child Protection on the Internet has also

published good practice guidance for providers of social networking and other interactive services. There are also several websites that have been created to increase education and awareness about online safety for children.<sup>279</sup>

### *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 UK ICO has a broad range of enforcement powers and can issue severe penalties for breaches of the Data Protection Act 1998, including up to two years imprisonment and a maximum fine of £500,000.<sup>280</sup> 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.<sup>281</sup> The UK, as well as other European countries, is taking data protection law seriously, and service providers should bear this in mind. There have, however, been a couple of successful challenges against the ICO's monetary penalty decision.<sup>282</sup>

In social media enterprises, an even greater risk than identity theft or financial fraud exists. There are reported cases of users of social media have been exposed to emotional abuse and have been sexually assaulted, among other crimes. Attempts have been made to hold the social media enterprises themselves liable for not doing more to stop these abuses.

Precautions to detect likely criminal activity, to the extent practicable, and having social media policies or other types of employment agreements establishing 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 policies and other types of 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*).

Additional complications for social media enterprises can arise in connection with the data they possess about their users. Social media companies have often been the subject of subpoenas in connection with criminal prosecutions. Some companies, such as Facebook, Google, and Twitter, have even set up guidelines for requesting records.<sup>283</sup> In some instances, the companies have refused to comply with subpoenas by invoking the Stored Communications Act, which in its broadest sense, limits the type of information that can be disclosed by electronic communication or remote computing service. For example, in 2012, Twitter sought to quash a subpoena to turn over thousands of Tweets from a writer in connection with his involvement in the Occupy Wall Street movement.<sup>284</sup> The judge ordered Twitter to produce the records, saying that the writer did not have a reasonable expectation of privacy in the postings, comparing the Tweets to screaming out a window.<sup>285</sup> Despite Twitter appealing the order, the records eventually were produced in court.<sup>286</sup>

### *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, making them an attractive target to hackers. There have been a number of hacking attacks made on social media companies over the past few years. In December 2013, it was reported that over 2 million usernames and passwords were stolen in a hack from Facebook, Twitter, and Gmail.<sup>287</sup> Less than a month later, in January 2014, 4.6 million accounts were hacked in a Snapchat hack.<sup>288</sup> Both of these attacks followed the 2012 hack on LinkedIn of 6.5 million passwords.<sup>289</sup> It is clear that social media companies have become a prime target for cybercriminals.

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 indispensable to making sure policy is part of day-to-day procedure. At the same time, outreach to subscribers to let them know what to expect (and not expect) from the company will help subscribers defend themselves from spoofers, phishers, and similar would-be attackers.

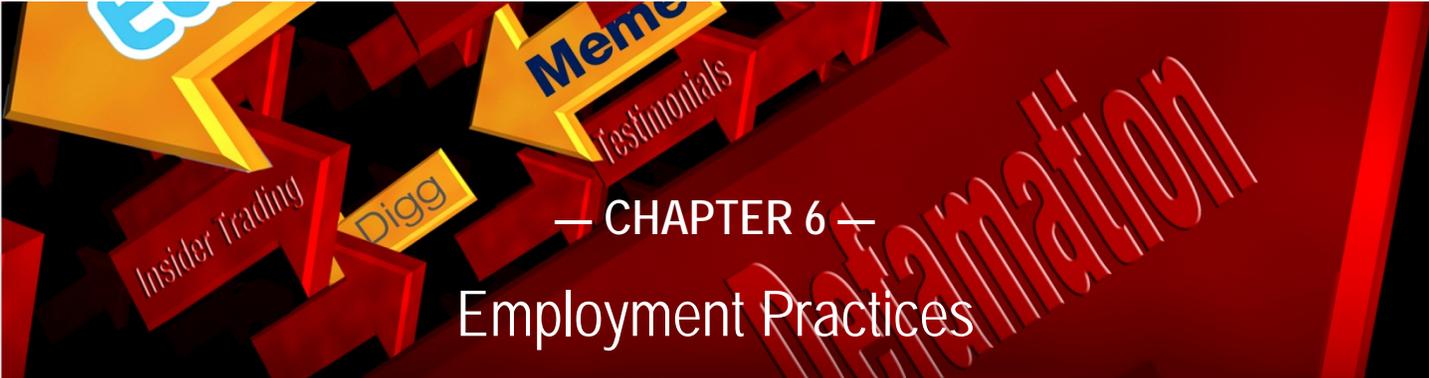
Also, like every company, social media companies should have plans for: the protection and secure disposal of personal data (including in hard copy); the implementation of major litigation holds; and response to the loss or theft of personal data (including, where required or appropriate, through notice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

### *Is the Company Properly Insured against Data Privacy Incidents?*

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

## Bottom Line—What You Need to Do

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



— CHAPTER 6 —  
Employment Practices

### Chapter Authors<sup>290</sup>

#### United States

[Sara A. Begley](#), Partner – [sbegley@reedsmith.com](mailto:sbegley@reedsmith.com)

[Eugene K. Connors](#), Partner – [econnors@reedsmith.com](mailto:econnors@reedsmith.com)

[Casey S. Ryan](#), Partner – [cryan@reedsmith.com](mailto:cryan@reedsmith.com)

#### United Kingdom

[Laurence G. Rees](#), Partner – [lrees@reedsmith.com](mailto:lrees@reedsmith.com)

[Carl De Cicco](#), Associate – [cdecicco@reedsmith.com](mailto:cdecicco@reedsmith.com)

[Ed Hunter](#), Associate – [ehunter@reedsmith.com](mailto:ehunter@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.<sup>291</sup> 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.<sup>292</sup> 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.<sup>293</sup>

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, tablets 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 rigeur 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, without the employer’s knowledge and approval, 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.<sup>294</sup>

### *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.<sup>295</sup>

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 application and vetting processes. 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.<sup>296</sup> 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 would 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.<sup>297</sup>

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 policy that establishes that such information would be used in the event of an investigation as a step toward demonstrating that the employer does indeed have such an interest. 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.<sup>298</sup>

#### *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.<sup>299</sup>

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<sup>300</sup>, such actions have multiplied over the past few years through the work of the HALDE<sup>301</sup>, 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<sup>302</sup>.

Another administrative body publishing guidelines and monitoring the use of social media, especially by recruitment agencies, is the data protection agency, the CNIL.<sup>303</sup> 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<sup>304</sup> composed a Charter on social media in which the signatories shall not use social networks to collect personal information on applicants<sup>305</sup>.

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.<sup>306</sup>

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.<sup>307</sup> 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.<sup>308</sup>

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.<sup>309</sup>

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.<sup>310</sup>

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 that an employee has engaged in unlawful activity.<sup>311</sup> Recently, the FTC revised the Guides Concerning the Use of Endorsements and Testimonials in Advertising.<sup>312</sup> 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 from accessing social media through use of the employer's equipment. A policy that is properly worded and well-publicised within the company 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 general 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.<sup>313</sup> Accordingly, employers should 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.<sup>314</sup> 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.

It is now an established principle that an employer can be liable for an employee's use of social media that discriminates against or harasses or threatens a co-worker, where the act of harassment or other discrimination is carried out by an employee during the course of their employment. However, whether such liability arises in a given situation will depend on the facts of the particular case. 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 includes the use of the employer's equipment may also be factors as to whether the employer would be vicariously liable. As an illustration of these principles, an employer was recently held to be vicariously liable for acts of harassment committed by two employees who posted comments about a colleague's sexuality on the colleague's Facebook page.<sup>315</sup> The conduct was committed in the workplace, during working hours and involved dealings between employees and their manager – therefore it was carried out "in the course of employment". The case also demonstrated that the question of whether an employer is aware that the conduct being complained of is happening (the employee in this case had reported the matter to the employer), or even condones or sanctions it, is irrelevant to the issue of vicarious liability.

Whilst the courts have readily held employers vicariously liable for acts of discrimination or harassment carried out during the course of employment, they have demonstrated a willingness to protect the employer's right to preserve its reputation when dealing with employees who post offensive comments on social networking sites outside of the workplace. In a number of recent cases, the Employment Tribunal has upheld the decision of employers to dismiss employees who expressed offensive views on social networking sites or through "chain" email correspondence.<sup>316</sup> In dismissing the employees' claims in these cases, the Tribunal has emphasised that, once an employee publishes offensive content, there can no longer be any reasonable expectation that the comments will be kept private, and therefore the employee may not be able to rely on their right to respect for private life that would otherwise be available under the Human Rights Act 1998.

Whether content published by or about an employee can be 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? Was the employer identifiable as employer of the employee? 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 (forexample, showing the employee to be well and active when the employee has informed the employer that they are unfit to attend for work)?<sup>317</sup>

As with monitoring, it is important that the employer collects uses any such content with due 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). That said this is unlikely where the employee had not taken any steps to draw the information to the employer's attention.

#### *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)<sup>318</sup>, 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<sup>319</sup>, 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<sup>320</sup>. 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.<sup>321</sup> 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, Facebook’s terms of use only prohibit the posting of content that “infringes or violates someone else’s rights or otherwise violates the law.”<sup>322</sup>

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<sup>323</sup>, 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.<sup>324</sup> 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.<sup>325</sup> 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.<sup>326</sup> 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<sup>327</sup>, 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 anti-discrimination legislation and 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. Although we are starting to see cases before the Employment Tribunals which test the boundaries of these protections, 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<sup>328</sup>, 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<sup>329</sup>.

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<sup>330</sup>.

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.

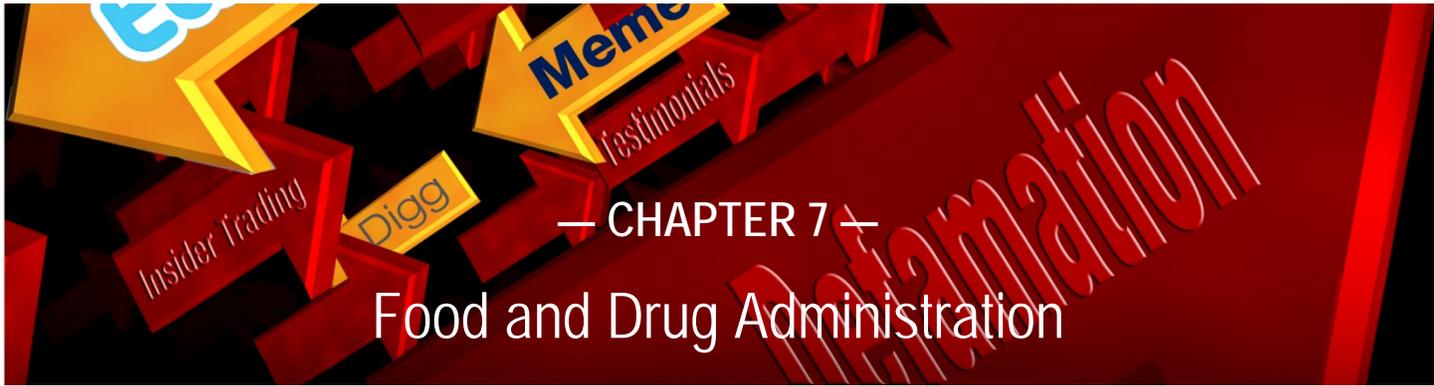
### Bottom Line—What You Need To Do

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 Authors<sup>331</sup>

[Colleen T. Davies](#), Partner – [cdavies@reedsmith.com](mailto:cdavies@reedsmith.com)

[Celeste A. Letourneau](#), Partner – [cletourneau@reedsmith.com](mailto:cletourneau@reedsmith.com)

[Tisha H.B. Schestopol](#), Counsel – [tschestopol@reedsmith.com](mailto:tschestopol@reedsmith.com)

[Kevin M. Madagan](#), Senior Associate – [kmadagan@reedsmith.com](mailto:kmadagan@reedsmith.com)

[Jennifer L. Pike](#), Associate – [jlpike@reedsmith.com](mailto:jlpike@reedsmith.com)

[Jillian W. Riley](#), Associate – [jwiley@reedsmith.com](mailto:jwiley@reedsmith.com)

## Introduction

Social media, the now-entrenched Internet and smart-phone phenomenon, enables decentralized, real-time communication among small and large groups of individuals, organizations and businesses. This fast-paced, interactive communication venue supports quickly evolving content that is available instantaneously and can be retransmitted exponentially to a broad audience.

The amorphous nature of social media, however, renders it unpredictable and elusive – two characteristics that can pose unique challenges, especially with regard to advertising, for regulatory authorities and the companies they regulate. One of these authorities, the U.S. Food and Drug Administration (“FDA”), has jurisdiction over manufacturers and distributors of medical products, including prescription drugs, biologics, medical devices, and emerging biotechnology products.

The following chapter explains why the FDA-regulated prescription drug and medical device industry has been very slow to adopt social media, even though other business sectors have fervently embraced social media as a product marketing tool. It also reviews FDA’s emerging policy on social media activities, and identifies potential risks associated with using social media to disseminate promotional messages about FDA-regulated prescription products. Suggestions on how to proceed in the current environment are also provided.

## Social Media in Action in FDA-Regulated Industry

Conversations through online social media communities among health care professionals and consumers about FDA-regulated products and disease-states are happening all the time. Sermo<sup>®</sup>, for example, one of the largest online physician social networks spanning 50 states, was launched in 2006 to provide a venue for physicians to

exchange observations in real-time about drugs, devices, and clinical issues.

Consumers are equally active on social media. A 2012 report by Pricewaterhouse Coopers LLP indicated that one third of U.S. consumers use social media sites such as Facebook, Twitter, and YouTube for health-related matters. These include forums for seeking information on specific diseases, about medical treatment, and for communicating opinions about drugs and devices.<sup>332</sup> Forty-five percent of

consumers said information found via social media would affect their decisions to seek a second opinion, and roughly 40% of consumers said they have used social media to find health-related consumer reviews.

It should come as no surprise, then, that manufacturers of FDA-regulated prescription products want to engage their customers through social media. Unfortunately, their ability to do so is hindered significantly by FDA regulations that were written before the social media phenomenon.

FDA-regulated companies are not avoiding social media entirely; many have a social media presence through company blogs, Facebook, YouTube, LinkedIn, and Twitter accounts. But prescription product marketing through social media largely has been restricted to create a more controlled environment. To the extent that these social media platforms are being used to disseminate promotional information about prescription products, the very features that make the media “social” – such as the ability to post a responding comment – have been disabled, and likely shall remain disabled, until FDA issues more definitive guidance about how FDA-promotional regulations will apply to social media.

### Current Regulatory Framework for Promotional Communications

FDA’s advertising regulations were developed at a time when advertising largely was limited to print, television, and radio advertisements, which are, for the most part, static cohesive swaths of information that are unchanged by others’ comments, reactions, or discussion. The underlying principles of these regulations require that promotional messages be truthful, non-misleading, and fairly balanced between the benefits and risks associated with a particular product.<sup>333</sup>

### Promotional Standards for Prescription Drugs – 21 C.F.R. § 202.1

Promotional pieces:

- Cannot be false or misleading in any particular.
- Must reveal material facts about the product being promoted, including facts about the consequences that can result from use of the product as suggested in the promotional piece.
- Should present information about effectiveness and

information about risk in a balanced manner.

When FDA evaluates a promotional message for compliance with 21 C.F.R. § 202.1 and other advertising standards, the agency looks not just at specific product claims and risk-related statements, but at the net impression of each message (*i.e.*, the collective message communicated by all elements of the communication). Characterization of data, broadening of approved indications, minimization of risks, and claims of superiority from improper comparisons to other products are not permitted.

In practice, this means that every promotional communication about a prescription product generally follows a scripted protocol for disclosing benefits and risks and providing access to all material safety and efficacy information about the product contained in the product’s prescribing information.

### Protocol for Promotional Communications (Examples)

- Benefit and risk information must be presented in clear, understandable, and non-technical language for the intended audience.
- The quantity and treatment of risk information must be comparable to the quantity and treatment of benefit information, including how it is conveyed.
- Except for “reminder” advertisements, every promotional communications must disclose the complete product indication and provide access to the product’s full prescribing information.
- Headlines and subheads should be consistent for both benefit and risk information.
- The communication must include material information (*i.e.*, information that is objectively important, relevant, or substantial to the target audience) about the product’s risks.
- Risk information should appear as an integral part of the main communication. (FDA will consider whether the placement of risk information interferes with readers’ perceptions of the relative importance or utility of the information.)
- White space (*i.e.*, background space between and around letters) must be considered at all times because it influences the prominence and readability

of text and will be considered by FDA when the agency evaluates a promotional communication.

When these, and other, advertising standards are applied to a new social-media technology (e.g., Twitter, Pinterest, Flickr, Facebook) – where communications are not static and there is loss of control over the presentation of information – applying regulatory standards can be challenging, to say the least.

How does a company ensure a fair and balanced presentation of important efficacy and safety information within a social media environment without interfering significantly with the discussion or social media stream? Given these standards, is it even possible for a company to fully utilize a social media platform as it was intended without removing the “social” aspect?

### FDA’s Emerging Social Media Policy

Since the inception of the Internet, and wide adoption and acceptance of social media, the FDA-regulated drug and device industry has been without formal FDA guidance or standards governing product promotion in these venues – resulting in confusion about how to interpret and apply traditional statutory provisions, regulations, and policies concerning advertising and promotional labeling to Internet- and social-media- based communications.<sup>334</sup>

In 1996, FDA held public hearings on Internet advertising and promotion, promising to issue regulations or guidance about this complicated issue.<sup>335</sup> This initiative, however, lost momentum and FDA went silent on the issues for the next three years.

In 1999, FDA informed its regulated industry that it would look at Internet issues on a case-by-case basis, while

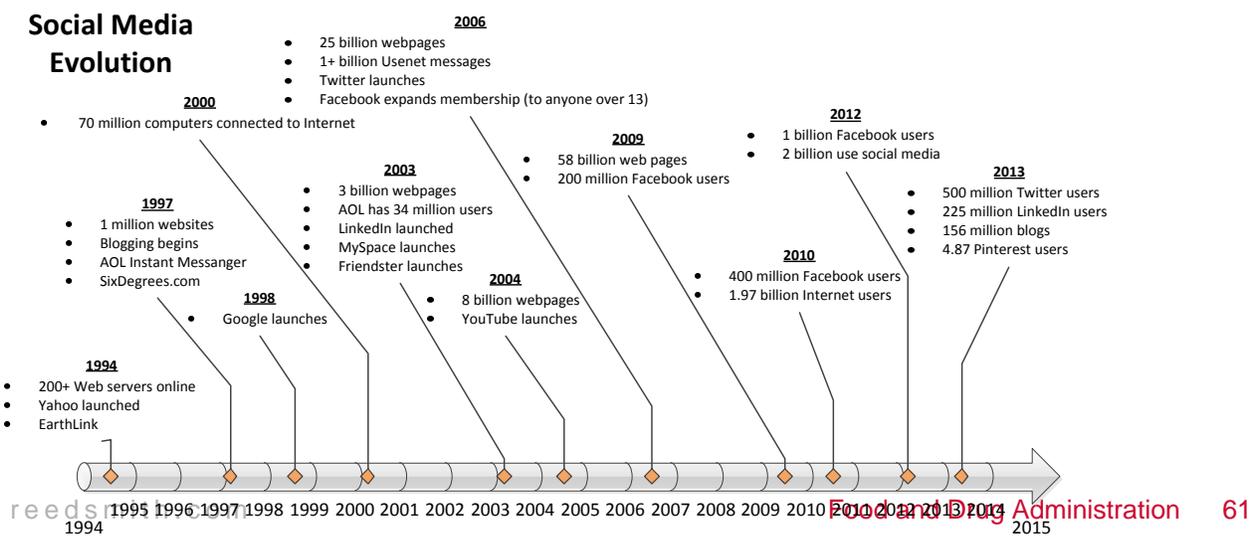
reserving the right to reevaluate the need for regulations in the future.<sup>336</sup>

Then a decade passed without much from FDA.

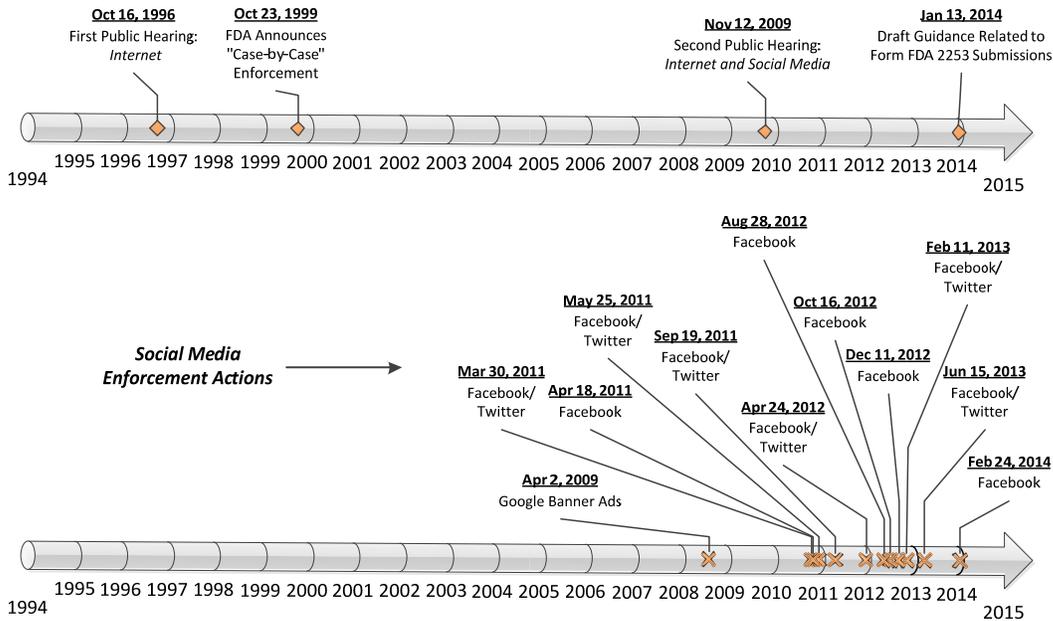
In 2009, FDA renewed its interest in addressing Internet communications and acknowledged the increasingly unique nature of the Internet and social media as a marketing tool and venue. Similar to the 1996 approach, the Agency held a public hearing about how the statutory provisions, regulations, and policies concerning advertising and promotional labeling for prescription products should be applied to product-related information on the Internet and social media. The hearing was very productive and triggered FDA’s current initiative to draft multiple guidance documents about this issue.

We know FDA has not lost interest in this topic and has been working diligently to issue guidance. But five years have now passed without much additional guidance. Indeed, from 2009 to early 2014, the Agency has merely reiterated a position it has held now for almost twenty years – that FDA’s advertising and promotion rules apply “regardless of the medium used.”<sup>337</sup> This lack of guidance creates uncertainty for companies and their promotional review teams whose responsibility it is to ensure that their company’s promotional materials comply with applicable requirements.

To be fair, in early 2014, FDA did issue a draft guidance instructing industry on how to comply with Form 2253 post-marketing submission requirements for dynamic materials and content in social media.<sup>338</sup> As explained later in this chapter, however, the draft guidance does not address myriad other unsettled issues that prevent many FDA-regulated companies from fully embracing social media as a promotional tool.



FDA Activity



Current Approach to Manage Risk

Without any formal guidance from FDA about how to apply FDA's advertising standards to social media, the drug and device industry must painstakingly scrutinize individual enforcement actions against companies that have created and used websites and social media to promote their products.

To date, these enforcement actions have clarified many things about FDA's policy on the use of websites and social media:

- *FDA will review any social media communication through existing FDA regulations.* The chart of enforcement actions listed at the end of this chapter a testament to this fact.
- The "one-click" rule does not exist; every promotional communication through social media must contain comprehensive product information, including safety information. The FDA-regulated drug and device industry once believed that FDA's requirement to provide comprehensive product information, including safety information, in promotional material could be satisfied if such information was directly accessible from a link in the original promotional piece (i.e., no more than one click away). This rule was commonly referred to as the "one click" rule. The rule was dispelled when FDA issued 14 enforcement letters in

2009 to companies for their failure to include sufficient risk information in Google banner advertisements.<sup>339</sup> These letters revealed FDA's thought on the "one click" rule, and sent shock waves throughout the industry, causing many companies to reassess their Internet marketing strategies. FDA subsequently stated that it "never had what some are referring to as a 'one-click rule.'"

- *Activities on social media pages, including Facebook and Twitter, are subject to scrutiny by the FDA.* In early 2014, for instance, FDA warned a drug company about statements the company made on its Facebook page.<sup>340</sup> The alleged violations themselves were straightforward and similar to more traditional advertising actions: failure to include risk information and omission of material facts. What makes this letter interesting is that the activity occurred on a social network. FDA has been issuing letters like these since 2011.
- The need to take corrective action will depend on whether and to what extent a company controls (or could control) a social media environment. FDA issued a Warning Letter to a company in 2011 because, among other things, consumers posted several disease-related testimonials on the company's Facebook page.<sup>341</sup>

- *Any communication through social media may be interpreted as a promotional activity.* In December 2012, FDA issued a Warning Letter to a dietary supplement company because the company, among other things, “liked” a post on its Facebook wall posted by a customer. FDA stated that the company’s promotional activities, including “liking” the Facebook post, suggested that the product was a drug because it is intended for use in the cure, mitigation, treatment, or prevention of disease.

These and other enforcement letters are listed in the chart at the end of this chapter. We will periodically update this chapter throughout the year.

## Regulatory Difficulties Presented by Social Media Remain Unresolved

### *Level of Control*

The use of social media is growing exponentially, and FDA-regulated industry cannot monitor every social-media communication related to its products. Industry does not want to be held liable for content that it does not generate or encourage. 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. But 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.

Although FDA’s recent draft guidance about Form 2253 submissions (discussed later in this chapter) allude to control as a factor considered by FDA when determining when and how to submit a Form 2253, industry needs more guidance from FDA about how control and responsibility relate to promotional activity in the social media context.

### *Transparency*

FDA and industry need to 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*

Industry wants FDA to account for the evolving nature of social media and space constraints. Stakeholders want guidelines or regulations regarding dissemination of risk information that are principle-based and applicable to multiple formats, social media included.

Despite FDA’s position on the one-click rule, many 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 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), companies are concerned that they may be held responsible for any statements made during the discussion, even by unrelated third parties. Industry is calling for FDA to permit companies to engage in online discussions without becoming responsible for all content, provided that its communications are truthful, non-misleading, and in accordance with any FDA standards for providing risk information. Many want FDA to provide them the freedom to determine whether and when to participate in or to correct information on third-party sites.

FDA has provided some guidance about how to respond to off-label questions on public social-media sites, but further clarification is needed about how a company may interact on third-party platforms.

### *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,<sup>342</sup> will impute knowledge and consent of an unapproved use to the manufacturer.<sup>343</sup> If knowledge and consent are imputed in this way, then the manufacturer could be held liable for promoting an unapproved use.

On December 27, 2011, FDA took some measures to address these concerns when it issued a draft guidance entitled “Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices.”<sup>344</sup> The draft guidance clarifies FDA’s policies on unsolicited requests for information, and includes some discussion about how a company should respond to unsolicited requests made through the Internet and social media.

Specifically, FDA makes the following recommendations to a company that chooses to respond to *public* unsolicited requests for off-label information about its product(s),

including those encountered through emerging electronic media.

- If a firm chooses to respond to the public request, the firm should respond only when the request pertains specifically to its own named product (and is not solely about a competitor's product).
- Representatives who respond to the request should clearly disclose their involvement with the company.
- The response should not be promotional in nature or tone.
- The response should convey that the question pertains to an unapproved or uncleared use of the product and state that individuals can contact the medical/scientific representative or medical affairs department with the specific unsolicited request to obtain more information.
- The response should provide specific contact information for the medical or scientific personnel or department (*e.g.*, e-mail address, telephone number, and facsimile) so that individuals can follow up independently with the firm to obtain specific information about the off-label use of the product through a non-public, one-on-one communication.

In sum, a response to an off-label request should be limited to providing the firm's contact information for appropriate dissemination and should not include any discussion of the off-label information.

If a firm responds in the manner described above, the draft guidance states that FDA "does not intend to use such responses as evidence of the firm's intent that its product be used for an unapproved or uncleared use." Enforcement decisions under the FDCA, however, 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 it views as being inconsistent with FDA guidance.

**Form 2253 Submissions**

FDA requires all prescription drug labeling and advertising to be submitted at the time of initial dissemination through an FDA Form 2253.<sup>345</sup> Because some social media communications (*e.g.*, real-time chat room discussions) are, in many regards, analogous to live discussions taking place between company sales representatives and health care professionals, many in the industry believe the Form

2253 reporting requirement for social media should be limited to some extent.

FDA addressed some of these concerns in a draft guidance instructing industry on how to comply with post-marketing submission requirements associated with promotion in the social media realm.<sup>346</sup> The draft guidance, issued in early 2014, outlines the types of social media activity that should be submitted for FDA review and the format of those submissions.

The critical element in determining whether FDA submission is required for product promotion on interactive social media is the degree of control or influence the drug company can exert over the website. If the company controls the promotion, regardless of whether it controls the entire site, the company needs to submit it to FDA for review. This control or influence standard extends to conduct of a drug company's employees and agents.

As to timing, the draft guidance says that submissions should be provided to FDA at the time of the initial dissemination and that the companies should provide monthly updates including a list of all sites where the company engages in interactive promotion. For password protected sites, the submissions need to include screenshots or other media to recreate for FDA what member-users see. Underscoring the limitations of existing mechanisms and processes for reviewing social media, these submissions should contain annotations to highlight for FDA which parts of the sites are interactive and thus subject to change.

**Next Steps at FDA**

FDA has promised repeatedly that it intends to issue multiple guidance documents on issues specific to the challenges presented by social media promotion.<sup>347</sup> In an interview published in April 2013 on the now defunct *Pharmalot* blog<sup>348</sup>, the Director of the FDA Office of Prescription Drug Promotion ("OPDP"), Thomas Abrams, stated that the development and issuance of guidance for social media was "among the highest of FDA's priorities."<sup>349</sup>

In response to the question of why it has taken the FDA so long to issue guidance documents, Abrams pointed to the concern that social media technology is constantly changing making it a moving target.

"It takes time because we follow good guidance practices and we want guidances that are well vetted and really address relevant issues, and stay relevant for a time period. It would be easier to come out with a

guidance in a shorter time that may not be relevant as technology changes. One thing we know is that we can't predict it, but we know technology is going to keep changing quicker and quicker. So we want this guidance to be applicable, regardless of which technology platform comes in the future or changes that existing platforms may make in the future."

Abrams was less clear when asked specifically for an actual date when the industry can look forward to formal guidance from the FDA.

"We are striving to make it as soon as possible. I'll be honest with you. As soon as we're able to issue these – we're not waiting for a deadline or we're not waiting for an event to occur. We are working very, very thoroughly and very hard – people are putting in extra hours ... And as soon as we can issue these, we will issue them. We are as anxious to issue them as industry is anxious to receive them. So we're not waiting for a deadline or a timeframe. As soon as they

are ready and we are happy they are good products that are well vetted and will remain relevant for a good time period, we will issue guidance."

Regardless, FDA has taken its first few steps in what has been (and will continue to be) a very long process within the agency to establish a framework for regulating social media, provide guidance to the industry, and find a way to adapt to emerging technologies.

Given that agencies such as the Federal Trade Commission (FTC) and Securities Exchange Commission (SEC) issued social media guidance in 2012 and 2013, and FDA issued the FDA Form 2253 submission guidance in early 2014, it seems likely that FDA will issue at least one additional social media guidance document in 2014, but some skepticism is warranted.

Indeed, the prescription drug and device industry remains today in the same position it's been in for the past two decades: anxiously waiting for formal guidance from FDA.

### Bottom Line—What You Need To Do To Mitigate Risk

Until FDA issues formal guidelines or promulgates new regulations governing the Internet or social media, assume that FDA will review any social media communication through existing FDA regulations.

Assume that all activity on social media networks, including Facebook and others, will be scrutinized by the FDA.

Develop policies governing employee use of social media.

Closely monitor and enforce these policies.

Closely track FDA warning and untitled letters to identify and avoid the mistakes your peers make when they communicate through social media.

Participate in FDA meetings open to the public and provide FDA with information when requested.

Pay attention. FDA's Internet and social media 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.

Consider following FDA draft guidance documents even though these guidance documents may be revised before they become final (*e.g.*, FDA's draft guidance entitled "Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices").

## Other Considerations About Social Media – Not Related to Promotional Activity

### Adverse Event Reporting

- Adverse event reporting regulations could be interpreted in a way that would require a company to monitor social media sites, and investigate adverse event information learned from such sites.<sup>350</sup>
- 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. FDA itself has been soliciting contractors to provide real-time analyses of online consumer messages related to FDA-regulated products.

### Mobile Medical Devices

- FDA's regulation of mobile medical devices is evolving. FDA's regulation of mobile medical devices might impact your company's approach to social media.

## FDA SOCIAL-MEDIA ENFORCEMENT ACTIONS

Company	Date	Key Issue	Citation
Institut Biochimique SA (BSA)	February 24, 2014	The Facebook webpage was deemed false or misleading because it made representations about the efficacy of Tirosint, a black box drug, but failed to communicate the full product indication or <i>any</i> risk information.	<a href="http://www.fda.gov/downloads/Drugs/Guidance/ComplianceRegulatoryInformation/Enforcement/ActivitiesbyFDA/WarningLettersandNoticeofViolationLetters/PharmaceuticalCompanies/UCM388800.pdf">http://www.fda.gov/downloads/Drugs/Guidance/ComplianceRegulatoryInformation/Enforcement/ActivitiesbyFDA/WarningLettersandNoticeofViolationLetters/PharmaceuticalCompanies/UCM388800.pdf</a>
Various Companies	June 15, 2013	FDA issued a series of Warning Letters to companies making claims related to the prevention and treatment of diabetes for unapproved drugs and devices.  FDA advised each company to "review all the information on your websites, including testimonials, social media websites (e.g., Facebook and Twitter), product labels, and other labeling and promotional materials for your products to ensure the claims you make are not in violation of the FD&C Act. It is your responsibility to assure compliance with all requirements of federal law and FDA regulations."	Example:  <a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm361849.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm361849.htm</a>

Oasis Consumer Healthcare	February 11, 2013	FDA issued a Warning Letter to Oasis, stating that Oasis' claims on its website, as well as claims on its Twitter page and Facebook page, fell outside the scope of the product's OTC monograph.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm339773.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm339773.htm</a>
AMARC Enterprises	December 11, 2012	FDA issued a Warning Letter to AMARC Enterprises, a dietary supplement company, because the company, among other things, "liked" a post on its Facebook wall posted by a customer. FDA stated that AMARC's promotional activities, including "liking" the Facebook post, suggested that its dietary supplement Poly-MVA was a drug because it is intended for use in the cure, mitigation, treatment, or prevention of disease.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm340266.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm340266.htm</a>
Quincy Bioscience Manufacturing	October 16, 2012	Quincy received a Warning Letter from the FDA in which the FDA stated that Quincy was promoting its products as drugs without an NDA. Therefore Quincy was promoting an unapproved drug in violation of the Food, Drug, and Cosmetic Act. FDA pointed to claims made by Quincy on both Quincy's website and on Facebook.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm324557.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm324557.htm</a>
Trinity Sports Group	August 28, 2012	FDA issued a Warning Letter to Trinity stating that Trinity was promoting its products as drugs without drug approval in violation of the Food, Drug, and Cosmetic Act. In addition to making claims on its website, FDA pointed to claims made on Trinity's Facebook page, including statements made by Trinity in the "About" section of the Facebook page, and statements made on the Timeline section of the Facebook page. Additionally, FDA also observed therapeutic claims made by Trinity on its Twitter page.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm318392.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm318392.htm</a>
Vitality Distributing, Inc.	April 24, 2012	Vitality received a Warning Letter from FDA for promoting its caffeine product as a drug without FDA approval in violation of the Food, Drug, and Cosmetic Act. In addition to statements made on its website, FDA also cited Vitality for posting on its Facebook and Twitter pages links to a third party article which made claims about the therapeutic effects of caffeine.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm301669.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm301669.htm</a>
Fatigued to Fantastic	April 18, 2012	FDA issued a Warning Letter to Fatigued to Fantastic stating that the company was making therapeutic claims about its products, which were not approved by the FDA. Fatigued to Fantastic was therefore promoting an unapproved drug in violation of the Food, Drug and Cosmetic Act. FDA also cited the company for including links on its Facebook page to its website, where the improper claims were made.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm301795.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm301795.htm</a>

Nature's Rite	September 19, 2011	Nature's Rite received a Warning Letter from FDA because it was promoting its products in such ways as to cause the products to be drugs. Because FDA did not approve the products, Nature's Rite was promoting an unapproved drug in violation of the Food, Drug, and Cosmetic Act. In addition to claims made on its website, FDA also noted a post made by Nature's Rite on its Facebook page in which the company made a therapeutic claim about its product.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm273464.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm273464.htm</a>
Cellular Rx	May 25, 2011	Cellular Rx received a Warning Letter from FDA for making therapeutic claims about its products. The claims established that the product was a drug, but the products did not have FDA approval. Therefore, Cellular Rx was promoting an unapproved drug in violation of the Food, Drug, and Cosmetic Act. FDA noted several testimonials posted on Cellular Rx's Facebook page that made disease claims.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2011/ucm256922.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2011/ucm256922.htm</a>
AloeElite	March 30, 2011	FDA issued a Warning Letter to AloeElite stating that the company was making therapeutic claims about its products, which were not approved by the FDA. AloeElite was therefore promoting an unapproved drug in violation of the Food, Drug and Cosmetic Act. In addition to claims on its website, FDA also pointed to a therapeutic claim in the "About" section of AloeElite's Facebook page.	<a href="http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm253987.htm">http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm253987.htm</a>
Various Companies	April 2, 2009	FDA issued enforcement letters on April 2, 2009 to 14 companies for their failure to include sufficient risk information in Google banner advertisements.	<a href="http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticesofViolationLetterstoPharmaceuticalCompanies/UCM055773#">http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticesofViolationLetterstoPharmaceuticalCompanies/UCM055773#</a>



## Chapter Authors

[Andrew L Hurst](mailto:ahurst@reedsmith.com), Partner – [ahurst@reedsmith.com](mailto:ahurst@reedsmith.com)

[Erin Felix](mailto:efelix@reedsmith.com), Associate – [efelix@reedsmith.com](mailto:efelix@reedsmith.com)

[Daniel Z. Herbst](mailto:dherbst@reedsmith.com), Associate – [dherbst@reedsmith.com](mailto:dherbst@reedsmith.com)

[Joelle E.K. Laszlo](mailto:jlaszlo@reedsmith.com), Associate – [jlaszlo@reedsmith.com](mailto:jlaszlo@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, and to supplement these guidelines over time.<sup>351</sup> 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.

As each government agency adopts policies and guidelines for the use of social media in order to manage behavior 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 their contractual obligations or government 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.<sup>352</sup> 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.<sup>353</sup> 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

Companies and individuals that are subject to civil or criminal investigations are frequently confronted with information derived from social media. Social media users create a staggering amount of data that government investigators routinely harvest in investigating civil or criminal culpability of individuals and their employers and utilize the resulting evidence in criminal or civil enforcement proceedings and prosecutions. This vast social media data pool includes several useful data points for investigators, including, among other things, the users' contacts and affiliates, likes, dislikes, and tastes, habits and preferences, and real time location data. Law enforcement agencies are highly attuned this wealth of investigative data, and investigators routinely mine social media for leads and evidence in investigations. See *Role of Social Media in Law Enforcement Significant and Growing* (7/18/2012) available at <http://www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1342623085481181> (noting that in July 2012, more than 80% of government investigations include some form of social media and that the number is growing).

Government agencies recognize that significant useful information may be *publicly available* on social media through a click of the mouse. See U.S. Dep't of Home Sec., *Privacy Impact Assessment for the Office of Operations Coordination and Planning: Publicly Available Social Media Monitoring and Situational Awareness Initiative 3* (April 1, 2013) [https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy\\_pia\\_ops\\_NOC%20MMC%20Update\\_April2013.pdf](https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_ops_NOC%20MMC%20Update_April2013.pdf). A somewhat recent example of government investigative use of social media involved antivirus company founder, John McAfee. In December 2012, McAfee, was under investigation for alleged death of a neighbor in Central America. Rather than answer the authorities investigation, McAfee went into hiding. When an iPhone photo of McAfee containing GPS location information was posted on a publicly available blog, law enforcement harnessed the lead, and McAfee found himself in a Guatemalan prison. See *How smartphone led to John McAfee's capture* (Dec. 6, 2012) <http://www.cbsnews.com/news/how-smartphone-led-to-john-mcafees-capture/>

Courts have held that limited Constitutional and statutory protections proscribe collection of data publicly disseminated by a social media user under the

"reasonable expectation of privacy standard" set forth by the U.S. Supreme Court in *Katz v. U.S.* One court recently held that Twitter must produce user information in response to a criminal subpoena. *See People v. Harris*, Case No. 2011NY080152, 2012 WL 2533640 (N.Y. Crim. Ct. June 30, 2012). In *Harris*, the court denied Twitter's motion to quash a subpoena to obtain a user's information, email address, and posts for a certain time period. Although Twitter argued that the user owns his tweets, the court held that users do not have standing to object to the criminal subpoena because the user has no proprietary interest in the information, nor does the user have a reasonable expectation of privacy in information shared with third parties. "There can be no reasonable expectation of privacy in a tweet sent around the world." *Id.* at \*3. The court concluded that "[s]o long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary." *Id.*

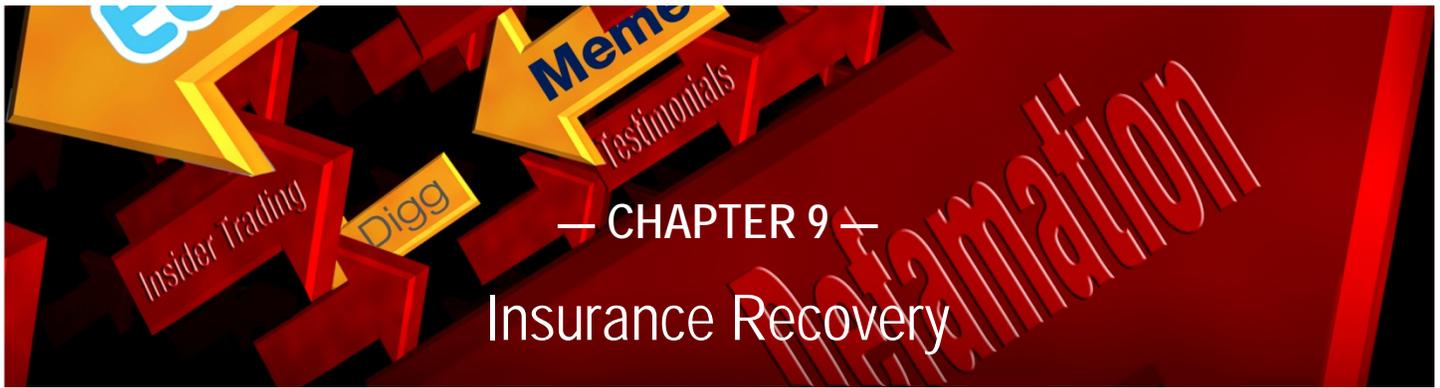
Government enforcement agencies often mine social media data for investigations through investigative subpoenas or search warrants to social media companies or internet service providers.. Although the practice has been challenged, principally under the Communications Act ("SCA") of 1986,<sup>354</sup> courts have been loath to limit the tools available to the government in conducting investigations when it comes to social media data that is intentionally disseminated by users.<sup>355</sup> The SCA requires government investigators to obtain a court order upon proof of "specific and articulable facts showing ... reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." See 18 U.S.C. § 2703(d).<sup>356</sup> Other basic information such as user names may be obtained with an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. § 2703(b)(1)(B)(i).

In all, the government has a robust set of investigative tools to access the vast amounts of social media data. Much of the data pools are made publicly available or publicly disseminated by users themselves, while other information may require the government to take additional procedural steps. Companies must understand the breadth of data available of social media and set appropriate social media policies and procedures pertaining to records management and document retention. (*See Volume 1, Chapter 8 – Litigation, Evidence and Privilege*). Moreover, companies also should establish policies and procedures as to the content and conditions of social media use related to company business for their employees and agents to ensure that information flow is

appropriately managed, and to prevent unwarranted disclosures before, during, and after government investigations. (*See Chapter 6 – Employment*). Finally, executives and all individuals using social media should remember the cardinal rule, think before you post.

### 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 Authors

### United States:

[J. Andrew Moss](#), Partner – [amoss@reedsmith.com](mailto:amoss@reedsmith.com)

[Carolyn H. Rosenberg](#), Partner – [crosenberg@reedsmith.com](mailto:crosenberg@reedsmith.com)

### United Kingdom:

[Peter Hardy](#), Partner – [phardy@reedsmith.com](mailto:p Hardy@reedsmith.com)<sup>357</sup>

## 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-related 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.<sup>358</sup>

For a number of years the insurance market in both the United States and the United Kingdom had been developing policies and coverage extensions to address the increased risk caused by the emerging use of technology in business. Initially, the policies tended to be customized and modular wordings rather than off-the-shelf products, and tended to reflect an insured's own perception of its exposure to this category of risk. So-called "cyberliability" policies have now evolved to the point where most insurers both in the U.S. and U.K. now offer off-the-shelf forms and endorsements focused on data protection and security and privacy liability, which may be tailored for specific industries and types of insureds. In this respect,

the U.S. and U.K. insurance markets are currently at somewhat different stages of development although a number of commentators anticipate that the U.K. will move closer to the U.S. model within a comparatively short time. The mandatory notification requirements for data breaches that exist under the laws of most U.S. states and laws and regulations that are being considered at the federal level and anticipated to be adopted in one or other form by U.K. regulators have crystallized an insurance market response. (See Chapter 5 – Data Privacy & Security.) The market is continuing to evolve but is now 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 offered in the market currently tends to focus on payment for the costs of compliance with mandatory notification requirements, the costs of providing initial relief to potential victims (including credit monitoring and insurance products), forensic investigation costs to determine the source of a breach or event, defense costs (including defending or responding to any regulatory

intervention), the costs of claims resulting from a breach (including damages and settlement costs), and payments to consumer redress funds. Although increasingly common additions to many insurers' suite of liability policies, Cyberliability insurance policy forms can vary from carrier to carrier, and 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, businesses that are particularly exposed to website content contamination and risks of defamation and copyright infringement are carefully scrutinized by underwriters.

Notwithstanding the moves made in recent years in the U.K. and outside of the U.S. in general, the insurance market remains less established for data protection and security and privacy insurance, not least because of the current reduced scope of mandatory reporting. But, as mentioned above, the U.K. and European landscape is changing and moving closer to, or perhaps exceeding the scope of, the U.S. model. Also, many businesses have a global reach that will require a risk assessment across a number of jurisdictions, including the U.S. Although it is not always true that the U.K. and European insurance market follows the lead of that in the U. S., there are obvious precedents, particularly in the area of directors' and officers' ("D&O") liability insurance, which demonstrate how this risk category might be expected to develop in the U.K. and Europe in the near future. The U.K. continues to witness greater regulatory activity, and the retail and financial institutions sectors in particular are developing the claims history necessary to fully understand the value and pricing of cyberliability coverage. 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 number of 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 U.K. and European market. Data protection and security and privacy coverage is available from most established insurers, and a company would be well advised to discuss with its brokers and insurance coverage counsel the particular exposures it may have 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 its 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 United Kingdom 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 or commercial general liability ("CGL") (for U.S. insureds), property damage and business interruption coverage, fidelity bond or commercial crime 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, they may also purchase stand-alone cyberliability 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 continue to grow both in frequency and scale.<sup>359</sup>

For example, a CGL policy issued in the U.S. 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 intangible or electronic data, while a coverage endorsement may specifically provide some coverage. "Personal injury" typically includes publication or utterances that violate an individual's right to privacy, or that are defamatory or disparaging. 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 U.S. and the U.K. 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" of coverage should a claim be made. Similarly, security or privacy breaches may be accompanied by a drop in the trading value of a company's stock, potentially giving rise to securities claims, which may be covered under a D&O policy or fiduciary liability policy, or a defamation claim may give rise to an employment-related claim, which may be

covered under an EPL policy. Accordingly, other policies should be examined to see if there are any potentially applicable exclusions or other restrictions that can be addressed when negotiating the coverage. Being proactive 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 in recent years, particularly in the United States. The first versions were difficult to assess given that claims were still emerging, few companies were purchasing them, 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 broadened in scope and 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 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 investigate breaches, secure legal compliance with a patchwork of laws and regulations, and 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 damages, judgments and settlements. The claims may include allegations of violations of privacy rights, unlawful or negligent disclosures of personal information, breaches of duties to secure confidential personal information under state and federal laws and regulations, breaches of duty, disclosures or fraudulent or criminal conduct by employees or others, infringement of intellectual property rights, unfair competition, defamation, violation of consumer protection statutes, and deceptive trade practices statutes.

The coverage may also include regulatory actions, lawsuits, and demands, including payments to consumer redress funds administered by regulatory agencies. Fines and penalties may also (but not uniformly) be expressly covered, subject to being insurable under the law of the relevant jurisdiction. 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 may constitute a Claim.

***A Broad Definition of "Loss."*** "Loss" should encompass a broad array of relief, including statutory fines and penalties where insurable, payments into consumer redress funds, as well as defense (including regulatory defense) and investigative costs.

***Narrowed Exclusions.*** Wherever possible, exclusions should apply only to that portion of a claim involving the excluded subject matter. Exclusions should also 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 and should be limited in scope to senior management (so as to not defeat coverage for the company or other employees in the event of a "rogue" employee). 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***

***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; cyberliability coverage for claims as a result of potential breaches of security and access to private data; CGL (in the U.S.) and property policies for potential business interruption claims; D&O and fiduciary liability 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. Although provisions differ by policy, it is not unusual for certain jurisdictions (including the U.K. and many U.S. states) to take a strict view of compliance requirements. For example, a fidelity bond policy will specify when the initial notice is to be provided, and a sworn proof of loss must be filed within a designated time period of reporting the initial loss. Cyberliability and D&O liability policies generally 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. Even though the claim may still be only a “potential” claim as opposed to an actual claim, the policy may still require strict reporting. Claims and potential claims should be contemporaneously 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, or if the insurer raises the potential for a coverage defense, 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 necessarily have a privileged relationship with an insurer, especially in a non-duty to defend situation (insureds also do not have a privileged relationship with their insurance brokers). Consequently, an insured would need to be very careful in sharing information with insurers. Confidentiality, common interest 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 proposes 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

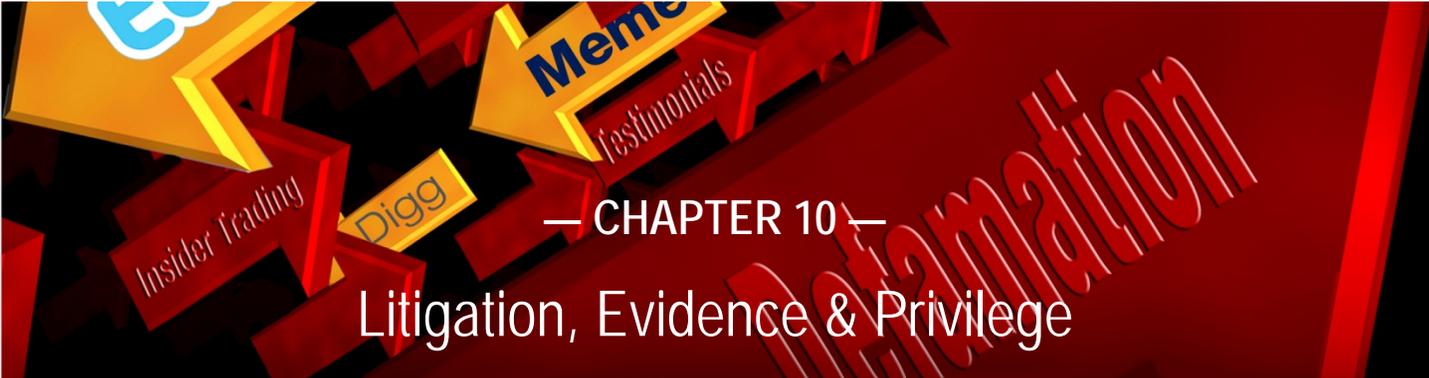
relationship throughout the claim process in a thoughtful and diligent way will typically put the insurer and insured in a better position to reach agreement, than if the insurer is not promptly brought “into the loop.”

*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 unusual for an insured seeking to recover a large loss from a “tower” of insurance coverage to litigate or engage in alternative dispute resolution (“ADR”) proceedings separately in the U.S. and the UK (or other jurisdictions), and commence both litigation and ADR 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<sup>360</sup>

#### United States:

[Alexander “Sandy” Y. Thomas](#), Partner – [athomas@reedsmith.com](mailto:athomas@reedsmith.com)

[Bonnie M. Mangold](#), Associate – [bmangold@reedsmith.com](mailto:bmangold@reedsmith.com)

#### United Kingdom:

[Emma Lenthall](#), Partner – [elenthall@reedsmith.com](mailto:elenthall@reedsmith.com)

[Louise Berg](#), Associate – [lberg@reedsmith.com](mailto: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, tablets, and personal computers. Social media postings often include details that the user would never disclose directly in a formal correspondence and certainly not to the boss of their company or to an opposing attorney if litigation were involved. Moreover, many people using social media do not realize that such postings often become a permanent record, even if the items are removed.<sup>361</sup>

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 the US:*

- In 2008, a minor accused her father of sexually assaulting her. On the minor's MySpace page, she made several posts alluding to the fact that she was not a virgin. However, when she filed the report against her father, she told the police that she was a virgin before her father began to sexually assault her. The court found that the MySpace statements could be used as impeachment evidence because they contained statements that were inconsistent with her prior statements, which directly went to the issue pending in the litigation.<sup>362</sup>
- In 2009, the defendant in a criminal case 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.<sup>363</sup>
- In 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 of stepping on GOD. I thank GOD 4 pot 2 calm down my frustrations n worries or else I will go beserk n shoot everyone...." Based on the evidence submitted by Starbucks, the court granted summary judgment in its favor.<sup>364</sup>

- In 2010, the plaintiff in a personal injury case claimed that injuries she sustained while performing duties in a Steelcase chair that collapsed rendered her unable to work, housebound, and unable to fully enjoy her life. Defense counsel pointed to plaintiff's Facebook and MySpace postings and photos, which showed that she still had the ability to enjoy her life. The court granted the defense's motion to compel production of this evidence and held that the private information sought from the social networking websites was material and necessary for the defendant's defense, that the plaintiff did not have a reasonable expectation of privacy in the material published on the social networking websites, and that the defendant's need for access to the information outweighed the plaintiff's privacy concerns.<sup>365</sup>
- In 2010, the plaintiffs brought a sexual harassment claim and the defendant sought to produce photographs from the plaintiffs' Facebook pages to prove that the plaintiffs did not suffer from severe emotional distress.<sup>366</sup>

*In the UK:*

- In 2010, in a trial involving allegations of sexual assault and attempted rape, the defence sought to rely on posts on the victim's Facebook page to show that she could not have had as clear a recollection of the incident as she claimed to have. The posts included "ATM remembers nothing" and "Filling in my memory would be very much appreciated there is very little of it ATM."<sup>367</sup>
- In 2011, an insurance company relied heavily on evidence from Facebook to show links between a group of people whom they alleged were involved in staging a series of accidents in order to claim damages for personal injury. The company submitted the 'friends' lists of various parties involved which showed a 'web' of connections. This, together with other evidence of dishonesty, helped to convince the judge that the accidents between people in the same local area with so many links and common relationships cannot have been a coincidence.<sup>368</sup>
- In 2011, a personal injury claimant alleged that a motor accident had left him wheelchair bound and too

traumatized to drive a car. The defendants submitted as evidence a picture of the Claimant on holiday in Italy which was taken from his Facebook page after the accident. He was standing next to his own car which he must have driven all the way there.<sup>369</sup>

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*). On the plus side, social media can be a useful source of evidence against a company's opponents in litigation, although care should be taken to ensure that no evidence is obtained by deception, and that ethical codes are complied with.

### *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 privilege and the work-product doctrine protection through public disclosure of confidential information. Below are a few examples:

- In 2010, the court granted the defendant's motion to compel discovery and ordered the plaintiff to turn over his Facebook and MySpace usernames and passwords to defendant's counsel despite plaintiff's claim that the abovementioned information was privileged. The court reasoned that "When a user communicates through Facebook or MySpace, however, he or she understands and tacitly submits to the possibility that a third-party recipient, i.e., one or more site operators, will also be receiving his or her messages and may further disclose them if the operator deems disclosure to be appropriate. That fact is wholly incommensurate with a claim of confidentiality. Accordingly, McMillen cannot successfully maintain that the element of

confidentiality protects his Facebook and MySpace accounts from discovery."<sup>370</sup>

- In 2010, the court held that the plaintiff waived her attorney-client privilege by virtue of her blog posts, gmail chats, and emails via which she had communicated with her attorney.<sup>371</sup>

As the above examples demonstrate, users of social media must be careful when disclosing personal or business information online in order to ultimately protect themselves from waiving the work-product doctrine or attorney-client privilege (or the equivalents in other jurisdictions) 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 online, and realize that certain postings will come back to haunt the employees and the company for which they work.

### *Social Media Use by Jurors*

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

*In the US:*

- In September 2010, a juror was removed from a jury for posting the following comment on her Facebook page, during an ongoing trial: "gonna be fun to tell the defendant they're GUILTY."<sup>372</sup>
- In December 2011, a juror in a criminal case Tweeted comments such as, "Choices to be made. Hearts to be broken. We each define the great line." The jury returned a guilty verdict, and

the trial court imposed a death sentence on the defendant. On appeal, the Arkansas Supreme Court reversed the trial court, holding that the defendant deserved a new trial because of the juror's unacceptable Tweets during the trial court proceedings.<sup>373</sup>

- In February 2012, a juror requested to be "friends" with the Defendant on Facebook. When the judge became aware that the juror had sent a friend request to the Defendant, the juror was promptly removed from the jury. After his removal from the jury, the ex-juror proceeded to post comments on his Facebook page, such as "Ha, ha, ha, I got out of jury duty."<sup>374</sup>
- In August 2013, a juror in a murder trial was removed from the jury for posting comments about the case on Facebook. Her comments reflected her belief the defendant was "presumed guilty," and she posted pictures of the courtroom hallway.<sup>375</sup>
- In October 2013, the California Supreme Court vacated the defendant's conviction because the jury foreman blogged about the case online on his personal blog.<sup>376</sup>

*In the UK:*

- In June 2011, juror Joanne Fraill was sent to prison for communicating on Facebook with a defendant who had just been acquitted. At the time of their online discussions about the case, the jury deliberations had not been completed and verdicts on other defendants were still to be returned. A new trial was ordered on the counts where verdicts awaited.<sup>377</sup>
- In July 2013, a fraud and money laundering trial had to be abandoned when a juror revealed to other jurors information that he had learned about the case on the internet. The wasted prosecution costs were in the region of £200,000.<sup>378</sup>
- In July 2013, a juror was held to be in contempt of court when he posted the following status update on Facebook during a trial for sex offences against children: "Woowoow I wasn't expecting to be in a jury Deciding a paedophile's fate, I've always wanted to Fuck up a paedophile & now I'm within the law!".<sup>379</sup>

As the above examples indicate, the use of social media by jurors during a trial may prejudice the outcome of a case if a juror leaks information about his or her perception of the case prior to the final verdict being rendered by all jurors, or reveals information about the case or the defendants that the juror has discovered online. 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 all parties involved. To prevent the above injuries, 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*

The English courts are beginning to allow lawyers to serve documents via social media where more traditional methods are considered to be inappropriate or insufficient.

In October 2009, the English High Court permitted service of an injunction via Twitter. In this case, which has become known as the 'Blaney's Blarney' case<sup>380</sup>, 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.

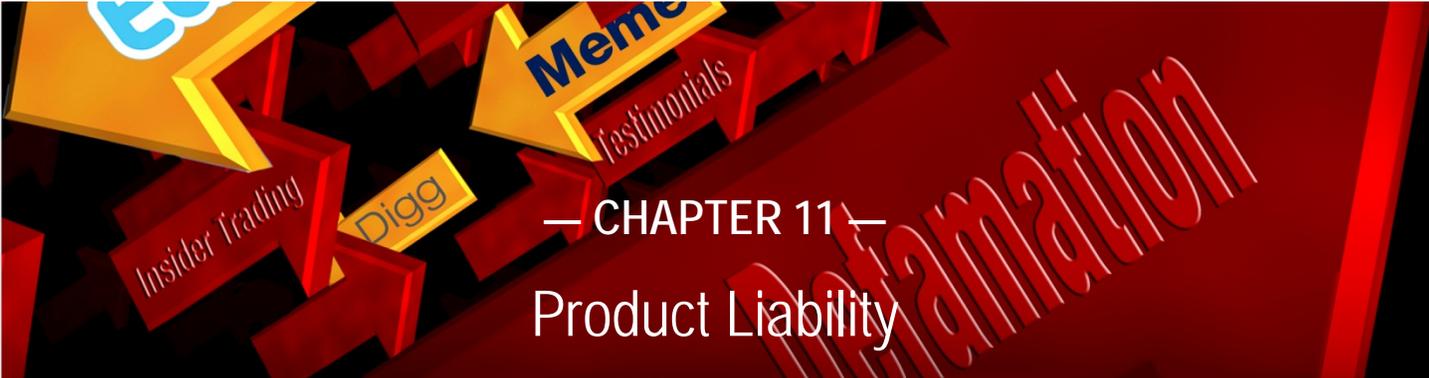
The English High Court also permitted service of a claim via Facebook in February 2012. In *AKO Capital LLP and AKO Master Fund Limited –v- TFS Derivatives Limited*<sup>381</sup>, the defendant applied to have one of its employees, Mr de Biase, added as a defendant. It was not clear whether Mr de Biase was still living at his last known address and so TFS applied to serve the claim via his Facebook account as well. Before allowing this method of service, the court requested assurances from TFS that (i) the Facebook account in question did in fact belong to Mr de Biase, and (ii) that he checked it regularly. TFS submitted evidence

from other employees who were friends with Mr de Biase on Facebook which showed that Mr de Biase had accepted a number of friend requests recently. The court accepted this evidence as providing both of the assurances it had requested and gave permission for service via Facebook. The documents were sent as attachments to a message to Mr de Biase's Facebook account.

As social media provides increasing scope for defamation and copyright infringement, more may 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. If this had not happened, 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<sup>382</sup>

[Antony B. Klapper](#), Partner – [aklapper@reedsmith.com](mailto:aklapper@reedsmith.com)

[Jesse J. Ash](#), Counsel – [jash@reedsmith.com](mailto:jash@reedsmith.com)

### Introduction

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

Companies that develop products utilize social media in a variety of ways, including internal and external company websites and blogs, pages on third-party sites such as Facebook, and other third-party sites that provide comments 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 defenses overall in the matter.

### The Need for a Social Media Marketing Program

Today, plaintiffs in product liability litigation often attempt to add allegations to their complaints based on information found online in an effort to bolster weak claims, defeat initial motion practice, and provide a backbone for boundless discovery. These allegations many times include accusations of improper promotion or misleading public. In today's marketplace, on-line advertisements and marketing campaigns are commonplace, in addition to editorials, studies, surveys, polls, and focus groups all found on the internet and related to a company's product. One only needs to put in a google search for their product's name to see the breadth of information written about the product—pro and against—and Plaintiffs' lawyers can easily do the same search. It is therefore of utmost importance in this day and age for a company to have an effective social media monitoring program designed to identify potential product liability issues. In enacting a program, companies must keep the following core issues in mind:

- Ensure that any social media statement complies with applicable regulatory requirements

Specific rules may govern what information a company can relay to the public or its customers. For example, pharmaceutical companies must abide by rules promulgated by the Food & Drug Administration ("FDA") when providing statements to patients or doctors through warning labels, package inserts, written correspondence, or visits to a doctor's office by a company's sales department—and this applies equally to promotional statements made on any online forum.<sup>383</sup> 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. For example, a company may have a blog or chat room where patients and/or doctors correspond with the company, and 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 (i.e., off label use).<sup>384</sup> Current FDA Guidance suggests

that such correspondence is now required to be submitted to the Agency as part of the postmarketing surveillance regulatory scheme to the extent that it exhibits a communication related to promotion of the product.<sup>385</sup> Companies that fail to adhere to this guidance may start to see “social media postmarketing surveillance regulatory violations” as an additional allegation to a plaintiffs’ boilerplate strict liability and/or negligence claim.

- Ensure that your online promotional statements are consistent with internal statements about the product

A plaintiff’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 plaintiff’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 plaintiff 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.

- Ensure that third-parties controlled by the company make statements online about your product that are consistent with your own promotion of the product

Paid speakers or Key Opinion Leaders (“KOLs”), and third-party marketers are common in product-driven industries. To the extent a company has control or exerts influence on these third parties, the company must ensure whatever messages are communicated by these parties online are consistent with internal statements and company promotional materials. KOLs are often highly sought after witnesses in product liability litigation. A plaintiff’s lawyer can easily create an effective demonstrative showing the KOL’s puffed statement about a product next to the amount he was paid by the company to opine about the product. These statements may be found, for example, in online power point presentations given at an industry conference or an online abstract of a study or an editorial—all publically available and ripe for use at a depositions or evidence at trial.

- Beware of Ghostwriting

If the company has editorial rights over the content of the site or exerts some level of control over an online author, plaintiff 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 plaintiff 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 favoring a competitor—would provide further arguments for a plaintiff 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.<sup>386</sup>

## Potential Causes of Action

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. As such, examples of causes of action where Plaintiffs may try to use social media statements by the company to their advantage in filing a product liability suit in the United States include:

- Negligent misstatement.
- Negligent promotion
- Negligent labeling
- Negligent marketing
- Strict liability
- Consumer fraud
- Breach of warranties
- Proposition 65 (CA) violations

## 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) and enacting a social media marketing program. Failure to do so can result in heightened exposure to legal claims, larger damages, and weakened defenses.

### 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](mailto:myoung@reedsmith.com), Partner – [myoung@reedsmith.com](mailto:myoung@reedsmith.com)

[James Boulton](mailto:jboulton@reedsmith.com), Associate – [jboulton@reedsmith.com](mailto:jboulton@reedsmith.com)

[Alexandra Nelson](mailto:maknelson@reedsmith.com), Associate – [maknelson@reedsmith.com](mailto:maknelson@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 20 million households (83 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 (53 percent via a mobile device), 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.

In this Chapter 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 2006 (the “Companies Act”) allows 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.

The Companies Act allows shareholders to communicate with a company by electronic means where the company

has provided an electronic address in a notice to call a meeting or in an instrument of proxy. Schedule 5 of the Companies 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). A company can also provide information to a shareholder by the use of a website if that person has agreed to the use of such website.

The Companies Act generally provides for the sending of documents in electronic form and by electronic means. Section 1168 of the Companies 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 Companies 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.

The Registrar of Companies (Companies House) for England and Wales, allows for the incorporation of companies to be undertaken electronically and for certain documentation to be filed electronically.

### *The Companies Act, 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 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 a 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 Financial Conduct Authority (the "FCA") 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 FCA pursuant to the Financial Services and Markets Act 2000 ("FSMA"). The FCA took over the responsibility for financial regulation from the Financial Services Authority (the "FSA") in April 2013.

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 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 FSMA is a criminal offence under section 25 of 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 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 FSMA, and/or civil liability under the market-abuse regime.

The FCA'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 FCA 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 FSMA. The FCA 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 FCA authorised person. The FCA 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 *FCA 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 FSMA includes 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 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 FCA's financial promotion rules. The rules for the financial promotion of securities can be found in chapter 4 of the *FCA's Conduct of Business Sourcebook* ("COBS") for savings and investments.

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

Of the 25 percent of the websites that failed to reach the “clear, fair and not misleading standards” of the FCA, 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 FCA 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. In 2013 the FCA issued a total of £472.3m of fines against over 40 firms representing a 52 percent increase on the £311.6m fines issued in 2012. In November 2013 the FCA also launched a review of 90% of all price-comparison websites, the results of which (and any resulting actions) are expected in 2014.

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 also 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.

Clive Gordon (formerly Head of the Conduct Risk Department at the FSA) gave a speech in September 2012 where he discussed online financial promotions and emphasised the need for banner advertisements to be stand-alone compliant; roll-over risk warnings and risk warnings requiring a person to ‘click’ the banner would not be sufficient.

1. Digital media stays in circulation longer than traditional media;
2. The media channel may not be suitable for all, certainly complex, products;
3. Risk information must be prominent and clearly displayed;
4. Must meet stand-alone compliance; and
5. Information must be full and sufficient.

**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 shareforum.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 FSMA and insider dealing rules under Part V of the Criminal Justice Act 1993 (“CJA”).

**Market Abuse**

Market abuse is a civil offence under sections 118 and 118A of FSMA. The FCA 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.

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 that 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.

While since March 2009, there have only been 23 convictions, since taking over from the FSA in April 2013, the FCA has continued to investigate insider dealing and pushed for prosecutions, resulting in a further seven individuals being prosecuted.

*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 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 Proxexis Plc. Krilov-Harrison had received inside information that Proxexis, 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 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 FSMA and MAR 1.8 is concerned with 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 FSMA.

### *Misleading Statements*

It is a criminal offence under s.397(1) of 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 former 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 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. 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 (iSoft had been engaged as a software supplier for the new £12.7 billion computer systems for the National Health Service). 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 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.

In June 2008, following a case at the Financial Services and Markets Tribunal, the FSA found that Winterflood and two of 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.

More recently the FCA has fined a US trader approximately £600,000 for manipulative trading known as 'layering' which uses an algorithmic programme to manipulate perceived buyer/seller interest in the market.

## 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 *FCA 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 *FCA 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 FCA 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 obligation to retain records also applies to information passing via electronic means. Legislation has previously passed on information passing via telephone but careful consideration also needs to be given to social networking tools, and posts to social networking sites which 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 FCA and is approved by a person authorised by the FCA, 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<sup>387</sup>

[Amy J. Greer](#), Partner – [agreer@reedsmith.com](mailto:agreer@reedsmith.com)

[Daniel Z. Herbst](#), Senior Associate – [dherbst@reedsmith.com](mailto:dherbst@reedsmith.com)

## Introduction

This chapter looks at the relationship between social media and the securities sector. A 2013 University of Massachusetts Study of the Fortune 500<sup>388</sup> found that 77% of Fortune 500 companies have an active Twitter account, leading all other social media platforms. This is an increase over 70% in 2012. The study found that in 2013, 171 companies (34%) had corporate blogs, showing the largest increase in use of this platform since the study began in 2008, and 348 companies (70%) are now on Facebook, a modest 4% increase since last year. But the largest companies are not alone in the securities sector. Issuers, brokers, investment advisors, investors, and the industry's primary regulator, the U.S. Securities and Exchange Commission ("SEC"), increasingly have embraced social media as a recognized a means of conducting business and engaging the marketplace. Wall Street financial institutions have Facebook pages, CEOs of Fortune 500 companies share information via Twitter, Instagram, and Pinterest, and the SEC, the Commodities Futures Trading Commission, and the Financial Industry Regulatory Authority ("FINRA") all maintain multiple Twitter feeds. Furthermore, new emerging markets have formed around the very medium of social media dubbed "crowdfunding."

With ever pervasive involvement of market participants, using social media requires careful consideration, supervision, and training to comply with the legal constructs from decades-old securities laws that demand timely, fair, and accurate dissemination of information. While the rewards of social media have the potential to be lucrative, those participating in the securities sector must be aware of the risks associated with instant, unfettered, and difficult to supervise conversations in the ever evolving regulatory landscape, which continues to receive significant regulatory scrutiny.

We begin by examining the use of social media by public companies to disseminate information to the market. Next, we consider how companies selling or marketing securities can use social media for advertising or promotion. Next, we look at social media in the context of raising private capital and the implementation of the JOBS Act. We then examine 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

### *Regulation FD and Making Information Public*

Recognizing that the availability of the Internet has broadened substantially and that, for example, more than 80 percent of mutual fund 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 and in some cases, through social media channels such as Twitter and Facebook.

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 purpose of Regulation FD is to avoid selective disclosure by promoting full and fair dissemination of information. The SEC now recognizes social media channels of distribution for required and other public information disclosures (either to meet regulatory obligations or in connection with individual securities transactions).

In an August 7, 2008 interpretive release followed by a disclosure interpretation issued on August 14, 2009, the SEC addressed the use of company websites for disclosures. This Guidance explains the general contours of Regulation FD 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. In these releases, the SEC made it clear that companies can use their websites for disclosure if their websites are a “recognized channel” for reaching investors when (1) the medium is a “recognized channel of distribution; (2) posting to the site disseminates information in a manner making it available to the securities marketplace in general; and (3) there is a reasonable waiting period for investors and the market to react to posted information. U.S. Securities and Exchange Commission, Release No. 34-58288, [Commission Guidance on the Use of Company Web Sites](#) 18, 25 (2008).

On April 2, 2013, the SEC updated its guidance in the form of a Report of Investigation indicating that Twitter, Facebook, and other social media channels could be used by public companies to disseminate material information without running afoul of Regulation FD. U.S. Securities and Exchange Commission, Release No. 69279, [Report of Investigation](#) (2013). Recognizing that social media is an extension of website, blogs, and RSS feeds discussed in the 2008 guidance, the Report of Investigation referred companies to the 2008 interpretive release and suggested that Reg FD’s “recognized channel of distribution” standards apply in the context of social media.

Critically, the guidance focused on the need of issuers to provide investors with *notice* of the particular social media

“channel” that the company intends to use to disseminate non-public information. The SEC noted that without notice, the investing public would have to keep pace with a “changing and expanding universe of potential disclosure channels.” The Report of Investigation noted that in order to provide such notice to investors of the social media channel, a company should include references to the channel in registration statements, periodic reports, or press releases, and on the corporate website(s).

While the April 2013 Report clarified that social media can be a “recognized channel,” it also noted that whether notice and use of the channel complies with Regulation FD and other securities laws must be evaluated on its own facts. The SEC’s Report of Investigation explained that dissemination of information on a corporate officer’s Twitter feed, absent advance notice to investors that the feed may be used to disseminate material non-public information may not qualify as an accepted method of communication and could run afoul of Regulation FD.

In another example, in January 2013, Zipcar filed a short 8-K with the SEC noting disclosures made by its CEO on his Twitter feed following the announcement that Avis would be buying the company for \$500 million. The filing was likely done because there was no prior identification of the Twitter feed as a channel of dissemination and because the transaction was subject to shareholder approval.

Based on this guidance, it is incumbent upon issuers whose officers or agents participate in social media to establish internal social media policies for its employees and officers so that the company speaks with one voice. Moreover, companies must provide outward facing materials on websites, press releases, registration filings, or periodic statements to inform investors where they can look to receive non-public information about the company in accordance with SEC guidance. Use of social media to disseminate information without required public notice could result in an enforcement investigation or action. As Regulation FD was designed to ensure fair dissemination of information and avoid selective disclosure, market participants that trade on selectively-disclosed information ahead of more broadly disclosed information potentially face more severe penalties.

## Advertising and Promotion in the Securities Sector

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.

The SEC and FINRA released an Investor Alert on June 12, 2013 concerning "pump and dump" stock emails. Financial Industry Regulatory Authority, [\*Inbox Alert—Don't Trade on Pump-And-Dump Stock Emails\*](#) (6/12/2013). The alert warned investors of similar advertisements made on "social media such as Facebook and Twitter, as well as on bulletin boards and chat room pages." Another recent Investor Alert warned of advance-fee scams using fake regulator Facebook websites and false broker identities. Financial Industry Regulatory Authority, [\*Well-Traveled Fraud—Advance-Fee Scams Target Non-U.S. Investors Using Fake Regulator Websites and False Broker Identities\*](#) (3/22/2012).

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 to avoid being lumped in with illegal scammers.

### ***Broker-Dealers and Their Registered Representatives***

Registered representatives ("RR") subject to Financial Industry Regulatory Authority ("FINRA") regulations need to obtain 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 FINRA 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 FINRA Rule 2111 (formerly 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:** FINRA members 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.

In December 2013, the SEC gave final approval to significant changes to FINRA's supervisory rules and, in March 2014, FINRA announced that new supervisory rules will become effective December 2014. . . See Notice <http://www.finra.org/Industry/Regulation/Notices/2014/P465941> In addition to reaffirming and consolidating prior rules, the new supervisory rules require "risk-based review" of additional types of incoming, outgoing, or internal communications and whether the member should require a review and update of existing policies and procedures. Such a risk based review may require members to reassess how the member uses social media and take additional steps to implement supervisory policies on use by its registered reps and other employees.

**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, 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.

**FINRA Issues "Sweep Letter" Seeking Social Media Data from Member Firms:** In June 2013, FINRA sent a targeted examination letter or "sweep letter" to its member firms inquiring into use of social media and the supervisory measures in place to oversee its use. FINRA sent the letter under authority of FINRA Rule 2210(c)(6), which allows FINRA to periodically "spot check" member firms' written and electronic communications. FINRA's sweep letter requested an explanation of the member's use of social media, identification of all media used by each member and who at each member firm controls the media, information related to the member's supervisory policies and procedures related to social media, member's compliance and training efforts related to social media, and a list with sales data for of the each member's top 20 producing representatives using social media.

Data from this sweep is likely to reveal that some members and their representatives failed to comply with applicable rules and potentially could lead to disciplinary actions. The sweep may also impact future FINRA rule-making or guidance in this area. More importantly, brokerage firms should conduct internal reviews of their social media policies and procedures to ensure not only that the procedures reflect current law but that the firm is implementing and training its registered representatives, supervisors, and compliance officers to adequately enforce those policies and procedures.

### *Registered Investment Advisers*

Statements of Registered Investment Advisors (“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’s Office of Compliance Inspections and Examination (“OCIE”) 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 the purpose of the communication 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 by the recommender. 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 a 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<sup>389</sup> 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 a RIA. It

stands to reason that if the SEC is on Twitter, then it is capable of finding compliance violations in social media.

### **Mutual Funds**

Following the OCIE Risk Alert, on March 15, 2013, the SEC's Division of Investment Management Division ("IM") sought to clarify filing requirements for mutual funds with respect to certain social media interactive content. U.S. Securities and Exchange Commission, [\*IM Guidance, Filing Requirements for Certain Electronic Communications, No. 2013-1\*](#) (March 2013).

Under Section 24 of the Investment Company Act and Rule 497 of the Securities Exchange Act, mutual funds must pre-file with FINRA all communications or advertisements that the fund intends to disseminate to the public. The applicability of these pre-filing rules with respect to social media or what IM describes as "interactive content" posted in real time interactive forums remained unclear. The industry tended to err on the side of being over inclusive, extensively filing all forms of potential interactive content with FINRA.

Prompted by the "flood" of interactive content filings, the 2013 IM guidance instructs mutual funds to use some discretion based on a set of prudential guideposts. The guidance suggests that the determination of whether to file certain interactive content as advertising is dependent upon "the content, context, and presentation of the particular communication" and "consideration of the facts and circumstances, such as whether the interactive communication is merely a response to a request or inquiry . . . or is forwarding previously filed content."

The IM guidance provides several sample illustrations on when filing is required and when filing is not required.

Broadly speaking, the guidance provides that interactive content ***should be filed*** in the following instances:

- Reference to a fund's performance or elements of a fund's performance ("Our quarter-end returns have exceeded our expectations!" or "The fund's performance rebounded in Q3!")
- Reference to the merits of investment in the fund ("Looking for dividends?" or "As you plan for retirement, consider our new fund").

Pursuant to the IM Guidance, ***pre-filing is not required*** in the following instances:

- Incidental mention of an investment company or fund family not related to the investment merits of the fund (“Fund X Family invites you to their annual benefit for XYZ charity.”).
- Incidental use of the word “performance” in connection without discussion of the elements of a fund’s return in the communication, including where the issuer refers a person to previously filed performance results. (“We update the performance of our funds every month and publish the results on <filed website link>”)
- A factual introductory statement forwarding or including a hyperlink to a fund prospectus or other information that was previously filed pursuant to Section 24(b) or Rule 497 (“The new ABC ETF Strategy Report is now available through <filed website link>”)
- A reference to general financial and investment information, such as basic investment concepts or economic, political, or market conditions without addressing the merits of the fund (“The election is over. What’s next for our economy? See our report analyzing the election <filed website link>.”)
- A response to an inquiry by a social media user that provides discrete factual, information that is not related to a discussion of the investment merits of the fund, which may direct the social media user to the fund prospectus or access to information filed with FINRA or to contact the issuer through a different medium. (INQUIRY: “Why are your funds such a large investor in ABC Manufacturer’s stock?” Fund’s posted response: “We respect your thoughts. As you know, ABC Manufacturer is found in many broad-market indices that our index funds are obligated to track so some of our index funds hold those shares as a result.” OR INQUIRY: “What are the fees and expenses for ABC Fund?” Fund’s posted response: “Information on the fund’s fees and expenses is available at <filed website link>. Feel free to contact us at 1-800-\*\*\*-\*\*\*\* for more information about this fund”)

While IM’s guidance provides useful guideposts for mutual funds that may curtail unnecessary interactive content filings, grey areas remain. Critically, funds would be wise to follow OCIE’s guidance and implement compliance programs that include social media policies to ensure principles of advertising rules, as clarified by IM, are integrated into firm policies. Moreover, due to the fact-sensitive nature of the inquiries, funds would be wise to implement robust training programs to implement and

execute social media policies, remain in compliance, and avoid enforcement actions.

### 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 in 2010, 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.

## Private Capital Raising

Social media presents both opportunities and regulatory risks to parties raising capital through private offerings of securities. Although general solicitations or advertising in connection with unregistered offerings traditionally has been proscribed, the Jumpstart Our Business Startups Act of 2012 (“JOBS Act”) provided limited exceptions to the general solicitation rule to allow the markets flexibility in raising capital and spark the economy. One key provision of the JOBS Act permits the use of “crowdfunding” or “crowdsourcing” in raising capital, subject to certain conditions. This section explores the applicability of social media to general solicitation rules and impact of the JOBS Act.

### *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. Exemptions include Regulation D, which permits issuers to sell securities in a private placement to an unlimited amount of “accredited investors” provided the issuer complies with the requirements of Regulation D. Accredited investors include individuals who meet certain minimum income or net worth levels, or certain institutions such as trusts, corporations or charitable organizations that meet certain minimum asset levels. Regulation D Rule 502(c) prohibits “any advertisement, article, notice or other communication published in any newspaper, magazine, or similar media or broadcast over television or radio, and any seminar or meeting whose attendees have been invited by any general solicitation or general advertising.” Social media likely would be considered “similar media” but the Commission has not addressed the issue.

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.

## *The JOBS Act*

### *(A) Lifting of the Ban on General Solicitation*

The Jumpstart Our Business Startups Act or JOBS Act was enacted with bipartisan support and signed into law in April 2012. The law encourages funding of small businesses by easing various securities regulations, and directs the SEC to promulgate rules to implement the regulations including rules regarding eased general solicitation requirements and crowdfunding/funding portals.

On July 10, 2013, the SEC voted to adopt final rules under Title II of the JOBS Act amending Regulation D and lifting the ban on advertisements and general solicitations in certain circumstances. U.S. Securities and Exchange Commission, Release No. 33-9415, [\*Eliminating the Prohibition Against General Solicitation and General Advertising in Rule 506 and Rule 144A Offerings\*](#) (2013). The final rule expands exceptions in private securities offerings from a broader category of private placement, including many offerings of interests in venture capital, private equity, real estate, hedge and other types of private investment funds so long as the solicitation is to an “accredited investor” as defined in Regulation D.

Under the final rule, issuers are required to “take reasonable steps” to verify that the investors are accredited investors and all purchasers of the securities must fall within one of the categories of persons who are accredited investors under an existing rule (Rule 501 of Regulation D) or the issuer reasonably believes that the investors fall within one of the categories at the time of the sale of the securities.

The SEC also voted to prohibit private placements by certain “bad actors” and propose for public comment a variety of rules that would limit opportunities for abuse of the new rule and enhance the ability of SEC staff to monitor activities pursuant to, and compliance with, the new rule.

To the extent issuers use social media in general solicitation or advertisements of private placements under the new rule, issuers must “take reasonable steps” to ensure recipients of social media solicitations and advertisements are only “accredited investors.” Such responsibility falls on issuers under the final rule and social media policies and procedures must be in place to ensure both the content and audience meet the regulatory requirements.

### *(B) Crowdfunding*

"Crowdfunding," also known as "crowdsourcing," is inherently a social media phenomenon and its regulation and proliferation may be a viable method to raise private capital in certain market sectors. Crowdfunding arose from networks of people pooling of small contributions to finance new enterprises. In response to the emerging development and with the intent to spur economic growth, Title III of the JOBS Act sets a framework for the SEC to develop and implement exemptions to registration requirements for private fundraising through crowdfunding.

The JOBS Act provides a framework to allow unregistered capital-raising through crowdfunding by the use of a registered brokers or, alternatively, through a crowdfunding intermediary known as a "funding portal." Funding portals must register as broker-dealers, but are held to lesser regulatory requirements. Funding portals would be prohibited from providing investment advice, soliciting sales, compensating employees based on sales of the offered securities, handling investor funds or securities, and engaging in other proscribed activities.

Title III limits crowdfunding to certain specific conditions including limits on aggregate capital raised and capital raised per investor, timing limits on portals and on transferability of crowdfunded securities, background checks for officers, directors, and significant shareholders in the enterprise, and filing, registration, and periodic reporting requirements.

In addition, the crowdfunding provisions proscribe advertising beyond directing investors to a registered broker or funding portal.

On October 23, 2013, the SEC proposed crowdfunding rules and solicited public comment. The proposed rules track the JOBS Act provisions and would permit, among other things, individuals to invest subject to certain thresholds based on the wealth and sophistication of the investor, limit the amount of money a company can raise, require companies to disclose certain information about their offers, and create a regulatory framework for the intermediaries that would facilitate the crowdfunding transactions.

Certain companies would not be eligible to use the crowdfunding exemption such as non-U.S. companies, companies that already are SEC reporting companies, certain investment companies, companies that are disqualified under the proposed disqualification rules, companies that have failed to comply with the annual reporting requirements in the proposed rules, and

companies that have no specific business plan or have indicated their business plan is to engage in a merger or acquisition with an unidentified company or companies.

The proposed rules would require companies conducting a crowdfunding offering to file certain information with the SEC, provide it to investors and the relevant intermediary facilitating the crowdfunding offering, and make it available to potential investors. Under the proposed rules, the offerings would be conducted exclusively online through a platform operated by a registered broker or a funding portal, which is a new type of SEC registrant.

Public comments have been generally critical of the proposed rules as inflexible and too constrained. The Commission continues to review comments and work towards either a finalized rule or an amended proposal, which many expect to be in spring/summer 2014.

Before the JOBS Act, in June 2011, the SEC entered a cease-and-desist order<sup>390</sup> against two individuals who attempted to "crowdsource" a purchase of the Pabst Brewing Company. The private owners of the Pabst Brewing Company sought to sell the company. The two defendants, whose backgrounds were in advertising, created a website, complemented by a Facebook page and Twitter account, called BuyBeerCompany.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.

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. Had the JOBS Act been in place, it is dubious whether the purported advertising scheme would have complied with federal securities laws. However, the Pabst Brewing enforcement action illustrates the social aspect of crowdfunding and the need for the SEC to implement regulations to reflect this emerging market trend. Private issuers interested in crowdfunding should proceed with caution in using social media to promote new sites and consult securities counsel on crowdfunding portals.

## 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*

Several 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 release in November 2013,<sup>391</sup> a registered representative and FINRA entered into a settlement following an investigation of alleged improprieties related to the broker's single Facebook post. The Facebook post responded to a Barron's article cautioning against buying a certain pharmaceutical stock at its then high price, based on some of the hurdles the Barron's author believed the company faced to bring a weight loss drug to market. The broker made the post on his Facebook wall with a comment describing the article as "idiotic" in addition to defending the drug and stating "there's no safer weight loss drug." His Facebook profile identified the broker as a financial planner at his member firm. At the time of the post, the broker owned 10,000 shares of the stock, worth about \$60,000, and about 33 of his clients also owned the stock, but he did not disclose these stakes in the posting, according to the FINRA settlement.

The settlement provided for a \$5,000 civil fine and 10-day suspension. The FINRA announcement states that "the broker posted a communication regarding a pharmaceutical company on a publicly available website that was exaggerated, not fair and balanced, and omitted the material fact that he and several customers owned shares of the company's stock." While FINRA's sanctions were de minimus, the case illustrates the challenges for brokers and members firms in navigating social media, even whereas here, the member firm had a written policy on the use of social media. Thorough training on social media policies is essential to avoid these pitfalls.

In another a recent disciplinary action,<sup>392</sup> 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.

#### *International Pyramid Scheme Using Social Media*

In *SEC v. Fleet Mutual Wealth*,<sup>393</sup> the SEC brought an emergency enforcement action in the U.S. District Court for the Central District of California to stop a fraudulent pyramid scheme by companies posing as a legitimate international investment firm on social media. The U.S. district court froze accounts holding money purportedly invested by U.S. investors with Fleet Mutual Wealth Limited and MWF Financial – collectively known as "Mutual Wealth."

The SEC complaint alleges that Mutual Wealth has been "exploiting investors through a website and social media accounts on Facebook and Twitter, falsely promising extraordinary returns of 2 to 3 percent per week for investors who open accounts with the firm." The SEC

claims that Mutual Wealth does not purchase or sell securities on behalf of investors, and instead merely diverts investor money to offshore bank accounts held by shell companies. Approximately 150 U.S. investors opened accounts with Mutual Wealth and collectively invested a total of at least \$300,000.

According to a March 2014 SEC press release, Mutual Wealth utilized social media channels such as Facebook, Twitter, YouTube, and Skype to make its investment pitch. In particular, Mutual Wealth maintained a Facebook account page and Twitter account which regularly posted status updates, making numerous online pitches and posts. Fraudulent comments populated Facebook wall posts filled with solicitations by the accredited advisors. Mutual Wealth also tweeted offering and announcements and invested in advertisements on other social media platforms.

According to the SEC, Mutual Wealth's website falsely denotes its headquarters in Hong Kong and its purported "data-centre" in New York – neither of which exist. Mutual Wealth also lists make-believe "executives" on its website, and falsely claimed in e-mails to investors that it is "registered" or "duly registered" with the SEC.

This unique case demonstrates the persuasive power of social media in reaching potential investors and the great potential to perpetuate fraud. Moreover, it shows that the regulators are highly focused on social media and have made policing its use by those in the securities sector a high enforcement priority.

#### ***Violation of Regulation FD***

In *SEC v. Black*,<sup>394</sup> 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 issued a press release projecting that second quarter earnings would be in line with first quarter earnings, the defendant sent emails 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.<sup>395</sup> 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*,<sup>396</sup> 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*<sup>397</sup> 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 Covansys. 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 revealed 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

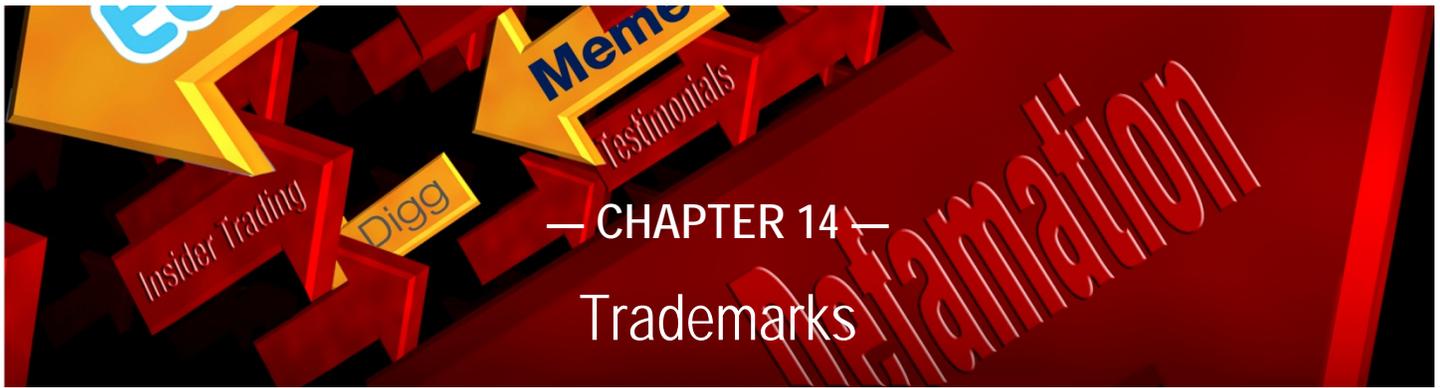
Before you decide to adopt social media as a form of communication and disclosure, you must ensure that the proper controls are in place. Whether it be material disclosures, advertising, or everyday business disclosures, your communications must meet regulatory requirements. For material disclosures, you must comply with Regulation FD. For advertising of transactions or services, you must obtain proper approval before using social media and must be sure 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. A good dose of preventative medicine would mean 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. In addition, it is wise to 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 Authors<sup>398</sup>

### United States:

[Darren B. Cohen](#), Partner – [dcohen@reedsmith.com](mailto:dcohen@reedsmith.com)

[Jillian L. Burstein](#), Associate – [jburstein@reedsmith.com](mailto:jburstein@reedsmith.com)

[Meredith D. Pikser](#), Associate – [mpikser@reedsmith.com](mailto:mpikser@reedsmith.com)

### Germany:

[Dr. Alexander R. Klett](#), Partner – [aklett@reedsmith.com](mailto:aklett@reedsmith.com)

### United Kingdom:

[Sachin Premnath](#), Associate – [spremnath@reedsmith.com](mailto:spremnath@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 with 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 or smartphone. 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 to increase brand awareness, they are also finding that unauthorized use of their trademarks, service marks, and trade names are emerging through these same channels.

First, we will examine trademark infringement occurring on social media platforms such as Twitter, Facebook, Instagram and Pinterest and how their respective policies deal with infringers. Next, we will examine the issue of impersonation on Facebook, Twitter, and Pinterest. 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*

Social networks such as Twitter, Facebook, Instagram, and Pinterest, to name a few, allow their members to adopt user names, personalized sub-domain names, and post pictures and hashtag links to content, all of which have the potential to create confusion as to source. There is little resolve to prevent an individual or entity from adopting a username or sub-domain name that incorporates another's trademark or personal name. Nor has the law caught up with issues involving re-posting or re-tweeting and resulting viral distribution of content that bears a trademark owned by another or impersonates a celebrity.

#### *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 400 million monthly visitors to twitter.com, and more than 200 million monthly active users around the world.<sup>399</sup> 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 of third-party "Twitterjacking" occurs when a member registers a username that is the trademark of another or a name belonging to a celebrity. When this occurs, the trademark holder may take action against the fake social media account if the account uses a trademark for a commercial purpose and consumer confusion is likely to occur as a result. For example, in September 2009, ONEOK, Inc., a natural gas company, sued Twitter for trademark infringement, alleging that the company wrongfully allowed a third party to adopt the handle twitter.com/oneok to post misleading information that appeared to be official statements from the company from which the unnamed third party tweeted information about the natural gas distributor.<sup>400</sup> The complaint alleged that the messages were misleading in that they were made to appear like official statements from ONEOK when, in fact, the company had no involvement in sending them. Over the course of a month, ONEOK unsuccessfully asked that Twitter terminate or transfer the unauthorized account. After the complaint was filed, however, the parties resolved the dispute and the account has since been transferred to the company.

While the use of corporate trademarks in fake Twitter accounts may give rise to a legal claim, not all companies

are choosing to exercise their legal remedies. For example, after the massive 2010 Gulf Coast oil spill, the fake twitter account @BPGlobalIPR emerged to satirize the company's public relations attempts.<sup>401</sup> With Tweeting comments like "The ocean looks just a bit slimmer today. Dressing it in black really did the trick! #bpcare," the account brought wide attention to the practice of "Twitterjacking" and just how devastating it can be to a company's global reputation. Rather than take the matter to court, however, the real BP made a statement through a spokesman that "People are entitled to their views on what we're doing and we have to live with those."<sup>402</sup>

A more complex situation arose for music retailer HMV, whose UK Twitter account was hijacked by employees who live tweeted the fact that they were being fired en masse.<sup>403</sup> Similarly, in January 2014, the Twitter account of Microsoft News was hacked by the Syrian Electronic Army leading to a tweet alleging that the company sells customer data to governments.<sup>404</sup>

While the HMV case serves to alert companies to have more robust internal policies on consumer-facing social network activity, third-party "Twitterjacking" such as that suffered by Microsoft is less easily controlled. 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 with regard to its brand or business affiliation may be considered a trademark policy violation. When there is a clear intent to mislead others through the unauthorized use of a trademark, Twitter will suspend the account and notify the account holder. When we determine that an account appears to be confusing users, but is not purposefully passing itself off as the trademarked good or service, we give the account holder an opportunity to clear up any potential confusion. We may also release a username for the trademark holder's active use.<sup>405</sup>

While Twitter provides such a policy and avails the public with a trademark violation report form, it ultimately remains the trademark owner's obligation to be hands-on about protecting its rights. Strategy in doing 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.

### Facebook

Facebook has over 1.15 billion monthly active users, allowing its members to connect with others, upload photos, and share Internet links and videos.<sup>406</sup> A recent eBiz MBA study ranked Facebook as the most-used social network by global monthly active users.<sup>407</sup>

Like Twitter, it too, has found itself defending claims of trademark infringement and has dedicated a large section of its terms of service to explain its intellectual property infringement policy as well as provide an intellectual property infringement report form. In addition to reserving the right to remove or reclaim a username upon complaint by a trademark owner,<sup>408</sup> Facebook's trademark policy provides, in part, that:

Facebook respects the intellectual property rights of others and is committed to helping third parties protect their rights. Rights holders will find information below 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.<sup>409</sup> With respect to enforcement of its policies, it appears that Facebook considers registered trademarks, as well as pending trademark applications and common law trademark ownership as sufficient to bring a claim of trademark infringement to the administrators of Facebook. However, the question of jurisdiction remains 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.

What we do know is that there have been relatively few lawsuits regarding the use of user names on both Twitter and Facebook. This may be due either to the fact that trademark infringement is not as pervasive a problem on social networking as it would appear, or, more likely, the policies established by Twitter and Facebook are effective in eliminating continued trademark infringement.<sup>410</sup>

Both Facebook and Twitter allow users to create personalized URLs, which allow a user's name to become part of the Web address. For example, a user may obtain the URL [twitter.com/username](http://twitter.com/username) or [facebook.com/username](http://facebook.com/username). In the United States, trademark disputes over domain names are specifically governed by the 1999 Anticybersquatting Consumer Protection Act and the Uniform Domain-Name Dispute-Resolution Policy, a system used by the Internet Corporation for Assigned Names and Numbers, which is the organization that assigns domain names. However, neither the Act nor the

Policy applies to social media sites which allow users to create personalized URLs.<sup>411</sup> As the law has yet to catch up with technology, trademark owners, rather than the network hosting the personalized URL, remain in the position to police the unauthorized use of their trademarks. Due to the vast nature of the internet and reach of social media, however, it remains extremely difficult for owners to maintain control over the use of their trademarks. Additionally, Facebook's policy for creating usernames does not explicitly warn or caution against the use of unauthorized trademarks.<sup>412</sup> Instead, it only links users to its administrative contact page.<sup>413</sup> In this context, it remains uncertain whether Facebook, under U.S. law and its current trademark infringement policy, will only stop uses of exact marks used within the Facebook platform, or whether it will also stop the use of unauthorized personalized URLs. If so, will use of the mark as only a username be sufficient to enact the policy, or must there be infringing content on the Facebook page? In the UK, the advent of personalized 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.<sup>414</sup>

Perhaps Facebook and Twitter should adopt a model similar to that of the Uniform Domain-Name Dispute-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.

### Instagram

Founded in 2010, Instagram is a free photo sharing application that allows users to take photos, apply a filter, and share it on the service or a variety of other social networking services, including Facebook, Twitter, Foursquare, Tumblr, and Flickr. In April 2012, Instagram was acquired by its then-rival, Facebook, and by June of 2013, it had more than 130 million users, posted over 16 billion photos, and received over 1 billion likes per day.

As a Facebook acquisition, Instagram's intellectual property policy is substantially similar to its parent company, as discussed above.<sup>415</sup> Also like Facebook and Twitter, Instagram utilizes hashtags to tag topics of interest or discussion forums, as well as connect users with similar interests. For example, an Instagram user, while eating at McDonalds, could theoretically take a photo of his Big Mac and fries and post it onto his Instagram account with the hashtags: #McDonalds #ImLovinIt #BigMac, #DietStartsTomorrow, which would then feed in a trending area of any Instagram user's homepage. Privacy settings on Instagram can arrange for the image as well as the related hashtags appearing in the Instagram post to automatically feed to other social networking sites, such as Facebook and Twitter.

It's clear that for a corporation that works hard to police its brands, forums utilizing hashtags can be both a blessing (to promote their product) and a curse (to police from infringement). In an effort to gain control, some companies are submitting applications to the U.S. Patent and Trademark office for federal registration of hashtags which describe their products. For example, in 2012, Stokely-Van Camp, Inc. applied for the mark "#WINFROMWITHIN" to be used by PepsiCo. in connection with its Gatorade brand.<sup>416</sup>

The creation of the hashtag as a social media tool has created a whole host of trademark-related questions from what types of hashtags may become registered trademarks to whether an individual or corporation can be liable for trademark infringement? For example, consider a scenario in which our Instagram user, above, visited McDonalds and posted a picture to his account with the above-mentioned hashtags. Now consider that the user has tens of thousands of individual followers from Instagram, Facebook, and Twitter combined. While this behavior would likely be considered nominative fair use, consider a further scenario where our user owns his own burger restaurant and uses the hashtags to generate traffic to his website or his actual restaurant. As seen here, the use of McDonalds' names and products may quickly cross the line between fair use and infringement.

So what is a mega-corporation like McDonalds to do? Should it trademark "#MCDONALDS" and other related or even potential terms that may be hashtagged just for good measure? While this is clearly one option, time will tell as more and more companies seek to police their intellectual property by obtaining trademarks that describe or promote their goods and services by the use of hashtags.

### Pinterest

Pinterest, a social media site that also launched in 2010, allows users to "pin" and share images onto digital pinboards that are linked to third-party websites, and has become one of the fastest growing social media websites of all time.<sup>417</sup> In February of 2012 alone, Pinterest drove more traffic to websites than Twitter, Google+, LinkedIn and YouTube combined.<sup>418</sup> While the site initially attracted mostly women to use Pinterest as a tool to plan weddings, save recipes, and post ideas for home decorating, corporate brands have taken notice and are finding ways to enter the Pinterest scene by posting infographics, educational content as well as product images.<sup>419</sup> Some major brands using Pinterest include General Electric's "Badass Machines" board, Adobe System's "Creative Workspaces" and Intel's "Geek Chic."

Pinterest, like Facebook and Twitter, has an intellectual property policy and provides a reporting method for trademark infringement claims:

Pinterest respects the trademark rights of others. Accounts with usernames, Pin Board names, or any other content that misleads others or violates another's trademark may be updated, transferred or permanently suspended.<sup>420</sup>

While Pinterest claims that it respects the IP rights of others, it does not, however, have a means by which an account can be verified as the "official" account for a particular brand. For example, a search for the clothing store "the Gap" does not reveal the official Gap Pinterest account, but rather a seemingly infinite list of pins, pinboards, and pinners created by individuals unrelated to the company. In order to locate the official Gap Pinterest board, a user would need to first conduct a search on Google, which would provide a link directly to the official Gap Pinterest Account. As a result of instances like this, "brandsquatting" on Pinterest affects 90 percent of top brands.<sup>421</sup>

In addition to "brandsquatting," celebrities and politicians are targets of fake Pinterest accounts. For example, during the 2012 United States Presidential campaign, a fake Pinterest account was made as a parody of former

presidential candidate Mitt Romney.<sup>422</sup> Pinterest complied with the Romney campaign's demand to rename the profile (which used Romney's full name), however, it did not give the original Mitt Romney name solely to the former GOP candidate. Instead, the name "Mitt Romney" links to at least nine different accounts named after the former candidate.<sup>423</sup> It remains to be seen just how seriously Pinterest will enforce its intellectual property policy in light of obvious "brandsquatting" by non-trademark owners.

**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..."<sup>424</sup> Similar "use in commerce" requirements exist for claims of unfair competition<sup>425</sup> and dilution.<sup>426</sup> 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? A December 2013 opinion from the Western District of Virginia involving the social media site 'LinkedIn' goes some way in clarifying the point. In this case, the Judge noted that "use in commerce" has been interpreted by the courts very broadly, and opined that "because the internet is an 'instrumentality of interstate commerce,' courts have repeatedly held that the unauthorized use of a trademark on the internet satisfies the 'in commerce' requirement."<sup>427</sup> Although the merits of the case are yet to be adjudicated at the time of writing, this court's opinion demonstrates that the creation of fictitious LinkedIn profiles (and perhaps profiles on Twitter or Facebook) may be actionable under the Lanham Act.

Under English law, as generally under trademark laws in the member states of the European Union that are harmonized under the EU Trademark Directive,<sup>428</sup> 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 service;
- The sign is identical to the registered trademark and is used in relation to similar goods and services and there is a likelihood of confusion by the public;

- 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.<sup>429</sup>

Under European Community trademark law, the CTM Regulation<sup>430</sup> 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,
- 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, or
- A sign is identical or similar to the CTM, the CTM has a reputation in the Community, and the use of the sign without due cause takes unfair advantage of, or is detrimental to the distinctive character of, the CTM

The European Court of Justice (ECJ) has held<sup>431</sup> 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. In fact, Twitter suggests in its intellectual property policy that users distinguish the account from that of the real company or business entity with a qualifier such as 'not', 'fake' or 'fan account'.<sup>432</sup>

The English courts have also addressed the question of jurisdiction.<sup>433</sup> 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 sites such as Facebook, Twitter, or LinkedIn, could result in different decisions depending on geographical coverage and demographic reach. Decisions in other European countries, such as Germany,<sup>434</sup> 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.<sup>435</sup>

While unfair competition law is not harmonized 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.<sup>436</sup> 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.<sup>437</sup>

**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 a violation of the Twitter Rules. Twitter accounts portraying another person in a confusing or deceptive manner may be permanently suspended under the Twitter Impersonation Policy.<sup>438</sup>

However, not all identical accounts will be removed. Twitter maintains that an account will not be removed if the users merely share a name but lack any other commonalities, or the profile clearly states it is not affiliated with or connected to any similarly-named individuals. As for accounts intended

to impersonate another, not all accounts with similar usernames or that bear a similarity in appearance (e.g. the same background or avatar image) are automatically in violation of the impersonation policy. In order to be deemed impersonation, according to Twitter, the account must also portray another person in a misleading or deceptive manner.<sup>439</sup>

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

- Avatar: The avatar should not be the exact trademark or logo of the account subject.
- Account Name: The name should not be the exact name of the account subject without some other distinguishing word, such as "not," "fake," or "fan."
- Bio: The bio should include a statement to distinguish it from the account subject, such as "This is a parody," "This is a fan page," "Parody Account," "Fan Account," "Role-playing Account," or "This is not affiliated with..."<sup>440</sup>

Nevertheless, countless celebrities have fallen victim to imposters who have acquired usernames of well-known personalities, including Tina Fey, Christopher Walken, and Kanye West.<sup>441</sup> The landmark case that brought this issue to light involved St. Louis Cardinals Manager Tony La Russa, who sued Twitter for trademark infringement for allowing an impersonator to send unauthorized and offensive messages under his name.<sup>442</sup> Specifically, he claimed that the unauthorized user made light of the deaths of two Cardinals pitchers, and the public was duped into believing that these statements were made by La Russa. The case 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.

Following the La Russa case, Twitter has created verified accounts, which is a tool developed to help establish authenticity of identities of key individuals and brands on Twitter.<sup>443</sup> An account that is deemed verified if a blue badge appears on the user's profile indicating that Twitter has been in contact with the person or entity the account is representing, and has verified that it is approved. Thus far, Twitter has awarded the 'verified' seal to more than 54,000 accounts.<sup>444</sup>

While acknowledging that it will not be verifying all accounts and will not accept requests for verification from the general public, Twitter states that it concentrates on verifying highly sought users in music, acting, fashion,

government, politics, religion, journalism, media, sports, business, and other key interest areas.<sup>445</sup> Ironically, however, while the drafter of the tweets sent from an account is not necessarily confirmed, many famous celebrities delegate the use of their Twitter account to their publicist or manager.

With respect to publically traded companies, transparency over the true number of authentic accounts on both Facebook and Twitter is likely to be ever more important as more and more corporations use their social network services to build their brand online.

### *Virtual Worlds*

Virtual worlds are another emerging area of unease. Developed through the application of user-generated content, members create avatars that exist in an online world. Second Life, one such 3-D virtual world where users can socialize, connect and create using voice and text chat, also allows users to create virtual products for sale online, using 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 a case from 2009 in the United States, Taser International, Inc. filed a trademark infringement claim against Second Life over the sale of unauthorized virtual versions of its electronic stun guns.<sup>446</sup> The lawsuit was later dropped, but the liability of Linden Lab, creator of Second Life, was debated in the media.<sup>447</sup> One question raised was why Linden Lab could not have been protected under the safe harbor provisions of the DMCA (*See Chapter 1 – Advertising*) or the CDA (*See Chapter 2 – Commercial Litigation*). After all, Linden Lab does not manufacture or sell stun guns, but merely provides the platform through which these “products” are offered for sale. The reason is because trademark infringement claims, unlike copyright claims, for example, are not covered by the DMCA or the CDA. Still, if one were to follow the logic of these statutes, it would seem that the creator of the product bearing the unauthorized trademark should be held liable, not the party who merely provided the platform. 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 unauthorized 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.<sup>448</sup> In the case of Herman Miller, the company allowed Linden Labs to continue using the Aeron name, provided that the virtual customers were charged a virtual premium price for their virtual premium chairs.<sup>449</sup> 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.<sup>450</sup> 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.<sup>451</sup>

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 unauthorized use of trademarks in the virtual world. However, real profits are, in fact, generated on such sites. Moreover, as noted by the Intangible Asset Finance Society:

It is undeniable that the virtual world population and the “real” life population overlap, and behavior in one medium can surely have an effect, adverse perhaps in this case, on the other. This type of activity may further prevent one from being able to fully exploit IP rights and build IP equity, in particular brand equity, by weakening, diluting and tarnishing trade mark rights or serving as a barrier to potential licensing opportunities and avenues.<sup>452</sup>

Other examples of virtual world trademark infringement include two cases involving the company Eros LLC. In one instance, Eros sued Leatherwood for the making and selling of unauthorized copies of its virtual adult-themed animated bed, using Eros' "SexGen" mark.<sup>453</sup> 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.<sup>454</sup> Eros had owned a pending application with the U.S. Patent and Trademark Office for the mark "SexGen" (which has since matured to registration)<sup>455</sup>, and a second plaintiff, DE Designs, owned a federal registration for the mark "DE Designs."<sup>456</sup> The plaintiffs were granted a judgment by consent, wherein it was ordered that the defendant:

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

As is evidenced by the above, businesses 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.<sup>457</sup> 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 Bitcoin, for example), with the global market for virtual goods expected to pass \$20 billion in 2015, and because increasingly younger generations are learning their first consumer experiences online.<sup>458</sup>

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, harmonized 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 above, 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.

Second Life, like Twitter and Facebook, has a policy in place to help avoid infringement and impersonation.<sup>459</sup>

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 or mislead other users regarding your identity or affiliation; or any name that Linden Lab determines in its sole discretion to be vulgar, offensive, or otherwise inappropriate.<sup>460</sup>

The policy adds that Linden Lab reserves the right to delete or change any account name that violates the above. In addition, an account cannot be transferred without the prior written consent of Linden Lab.

The policy further provides that:

In connection with Content you upload, publish, or submit to any part of the Service, you affirm, represent, and warrant that you own or have all necessary Intellectual Property Rights, licenses, consents, and permissions to use and authorize Linden Lab and users of Second Life to use the Content in the manner contemplated by the Service and these Terms of Service.

And that the user will not:

Impersonate any person or entity without their consent, or otherwise misrepresent your affiliation, or if you are an adult, impersonate a minor for the purpose of interacting with a minor using the Service.  
461

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

### *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.<sup>462</sup> 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."<sup>463</sup> The case settled.

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

### Bottom Line—What You Need To Do

It is of the utmost importance to have 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.



## Managing Risk Resulting from Assertions by Patent assertion Entities (PAEs)<sup>464</sup>

### Chapter Author

[Marc S. Kaufman](#), Partner – [mkaufman@reedsmith.com](mailto:mkaufman@reedsmith.com)

### Introduction

Risk resulting from patent infringement allegations has always been high in the United States. The emergence of the Patent assertion Entity (PAE) model has served to increase this risk. PAEs 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 PAE is to assert patents and generate revenue from licensing fees or damage awards assessed by courts. PAEs, 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 PAEs. This, combined with the aggressiveness of PAEs 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 PAEs. Recent patent assertions have targeted common internet marketing practices:

- The use of QR codes to direct a user of a mobile device to web content
- Putting a store locator on a web site
- Superimposing a facial image on an animated body image
- Placing static ads in a video stream
- Embedding a URL in a text message to direct a mobile device to web content

To be clear, the typical PAE revenue model is perfectly legal. PAEs can be venture capitalists purchasing patents on the open market for a return on investment, “privateers” who provide the resources to sue for patent infringement on behalf of the owner, innovators who have developed significant technology only to see it misappropriated by large companies without remuneration, or large IP aggregators, for example. However, the frustration and uncertainty caused by this business model has led to various changes in the common law and statutes.<sup>465</sup> Additionally, several states Attorneys General have addressed the issue by launching investigations into the practice of specific PAEs believed to be practicing anticompetitive tactics.

Notwithstanding the efforts noted above, the PAE business model, though, will likely remain legal and perfectly viable in the foreseeable future. Therefore, a good strategy for managing the risk presented by PAEs is necessary when doing business in the

United States. This article will avoid the discussion of visceral and emotional reactions to the PAE model in favor of articulating constructive approaches to managing risk and uncertainty.

It is important to understand the typical PAE value proposition. Most PAEs will offer a license that, while expensive, will likely be less than the costs of taking the PAE to trial and less than the cost of evaluating the patent in some cases. The proposition presented by the typical PAE is, "for X dollars, we (the PAE) 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 PAE 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 PAE 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, PAEs often utilize contingent fee attorneys and thus have little out-of-pocket expense. This imbalance is the foundation of the PAE revenue model.

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

- The PAE 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 PAE
- 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 PAE assertion becomes a less desirable opponent and thus eliminates some of the leverage of the PAE. The five key components to a successful resolution of an PAE 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 PAE assertion before beginning negotiation in earnest. PAE assertions range along a spectrum from "nuisance," in which the PAE does not have a strong legal position and is looking merely for a modest payment, to high risk, in which the PAE 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 PAE will likely disagree on the relative legal strength of the PAE 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 PAEs 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 PAE assertions have solid legal and factual bases and are best treated as such. Therefore, it is important to assess 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 PAE, its targets, its business model, and settlement terms. For example, has the PAE filed suit before? If so, what was the outcome and did the outcome affect the value of the asserted patents? What tactics has the PAE used for licensing/settlement? Who is counsel for the PAE 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 PAE 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 PAE 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 PAE. 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 PAE 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 PAE demonstrating that the PAE has risk as a result of potential invalidity and/or non-infringement. Also, if the damages analysis shows that the PAE 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 PAE. 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 PAE to file suit in a venue of the PAE's choice. Alternatively, it may be desirable to be proactive and put pressure on the PAE. 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 PAE is to file a Declaratory Judgment action in a venue of the target's choice prior to any suit being filed by the PAE. Whether litigation is filed by the PAE 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 PAE 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 PAE 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 PAEs 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 PAE’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 PAEs cannot be eliminated—at least not in the short term—many tactics can be used to reduce uncertainty and thus reduce PAE leverage. Reduced PAE leverage means reduced risk for the target. Potential targets of an PAE 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 PAE patent assertion models.

## — Biographies of Authors and Editors —



[Sara A. Begley](#), Partner – Philadelphia • +1 215 851 8214 • [sbegley@reedsmith.com](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto:p Hardy@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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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.



**[Celeste A. Letourneau](#)**, Partner – Washington, D.C. · +1 202 414 9260 · [mcletourneau@reedsmith.com](mailto:mcletourneau@reedsmith.com)

Celeste advises clients on FDA and health care regulatory, compliance and enforcement matters. Celeste specializes in advising clients on FDA regulatory and transactional issues related to pre-clinical and clinical trials; marketing approval; product labeling; manufacturing and distribution; advertising and promotion; pharmacovigilance, biospecimens, and FDA inspections and enforcement actions. Celeste also advises clients on a broad range of health care regulatory matters, including: Medicare coverage of routine costs and medical devices in clinical trials, HIPAA, and state regulation of manufacturers, distributors and health care providers.



**[Stacy K. Marcus](#)**, Partner – New York · +1 212 549 0446 · [smarcus@reedsmith.com](mailto:smarcus@reedsmith.com)

Stacy 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.



**[Mark S. Melodia](#)**, Partner – Princeton · +1 609 520 6015 · [mmelodia@reedsmith.com](mailto: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.



**[J. Andrew Moss](#)**, Partner – Chicago · +1 312 207 3869 · [amoss@reedsmith.com](mailto:amoss@reedsmith.com)

Andy is a member of Reed Smith's Insurance Recovery Group in the Litigation Department. Andy joined Reed Smith when the firm combined with Sachnoff & Weaver, Ltd. in March 2007. Andy concentrates his practice on the representation of companies and management as policyholders in insurance disputes involving directors' and officers' liability (D&O), professional and errors and omissions liability (E&O), data and network security and privacy liability (cyberliability), fiduciary liability, employment practices liability (EPL) and fidelity bond and commercial crime insurance. In addition, Andy counsels companies and management in the negotiation, evaluation, placement and renewal of D&O, E&O, fiduciary liability, employment practices liability, fidelity bond and commercial crime insurance.



[Kathyleen A. O'Brien](#), Partner – Century City · +1 310 734 5268 · [kobrien@reedsmith.com](mailto: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](mailto: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](mailto: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.



[Peter D. Raymond](#), Partner – New York · +1 212 549 0364 · [praymond@reedsmith.com](mailto:praymond@reedsmith.com)

Peter specializes in intellectual property and commercial litigation. He has tried bench and jury cases and argued appeals in the state and federal courts in New York and has appeared in courts and in administrative tribunals throughout the country. In particular, Peter represents clients in disputes involving false advertising, unfair competition, copyright and trademark infringement, trademark dilution, product disparagement, and invasion of rights of privacy and publicity. Peter has also lectured and acted as an expert witness in intellectual property and comparative advertising matters.



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



[Carolyn H. Rosenberg](#), Partner – Chicago · +1 312 207 6472 · [crosenberg@reedsmith.com](mailto: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](mailto:cryan@reedsmith.com)

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



[Alexander "Sandy" Y. Thomas](#), Partner – Falls Church/Washington, D.C. · +1 703 641 4276 · [athomas@reedsmith.com](mailto: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](mailto: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](http://www.ana.net)) and is the Chairman and founder of the Global Advertising Lawyers Alliance ([www.gala-marketlaw.com](http://www.gala-marketlaw.com)).



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



[Jesse J. Ash](#), Counsel – Washington, D.C. · +1 202 414 9449 · [jash@reedsmith.com](mailto:jash@reedsmith.com)

Jesse is a member of the Life Sciences Health Industry Group. His practice focuses on products liability litigation and he has extensive experience handling matters for an array of multinational companies in the pharmaceutical, medical device, health care and alcoholic beverage industries in both state and federal courts. Jesse has a strong background in electronic discovery, organizing and supervising numerous large-scale document productions for clients around the country, including all facets of the process from hold letters, to initial preservation and organization of discovery parameters, to the review and assessment for production, privilege and fact development. As a member of the Sedona Conference on Electronic Discovery, Jesse combines the unique experience gained while working at his prior discovery counsel boutique law firm, where he also had responsibility for the day to day management of the firm, with his long-time experience at Reed Smith, which puts him on the cutting edge of the electronic discovery industry.



[Tisha Schestopol](#), Counsel – Washington, D.C. · +1 202 414 9237 · [tschestopol@reedsmith.com](mailto:tschestopol@reedsmith.com)

Tisha joined Reed Smith in 2013 as counsel for the Life Sciences Health Industry Group. Previous to joining the firm, she was Senior Regulatory Counsel at Human Genome Sciences, where she provided health care and FDA regulatory and compliance guidance as the company pursued commercialization of its first product under a co-commercialization agreement with a large pharmaceutical manufacturer. She assisted in the development and monitoring of the corporate compliance program, including establishment of policies and processes related to health care professional interactions, compliance with transparency reporting, investigations, advisory boards, field exhibit and display requests, charitable contribution and grant review. She also advised on compliance with FDA requirements and guidance related to advertising and promotion.



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



[Jillian L. Burstein](#), Associate – Chicago · +1 312 207 2779 · [jburstein@reedsmith.com](mailto:jburstein@reedsmith.com)

Jillian is a member of the firm's Commercial Litigation Group.



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



[Christine Nielsen Czuprynski](#), Associate – Chicago · +1 312 207 6459 · [cczuprynski@reedsmith.com](mailto:cczuprynski@reedsmith.com)

Christine focuses her practice specifically in the area of data privacy and security, as well as telecommunications and marketing, as part of the firm's Global Regulatory Enforcement Group. Christine counsels clients on topics ranging from security breach preparedness and response, to SMS and email marketing campaigns. She provides regulatory advice on the Telephone Consumer Protection Act (TCPA) and the Fair Credit Reporting Act (FCRA). In addition to TCPA and FCRA compliance advice, Christine offers guidance on CAN-SPAM, COPPA, and U.S./EU Safe Harbor certification. She also has extensive litigation experience, defending her clients against privacy-related class actions, such as those involving the TCPA and data security breaches.



[Erin Felix](#), Associate – Washington, D.C. · +1 202 414 9273 · [efelix@reedsmith.com](mailto:efelix@reedsmith.com)

Erin is a member of the Global Regulatory Enforcement Group and focuses her practice on government contracts and grants. Erin's practice includes representing prime and subcontractor clients in negotiations; disputes, claims, and bid protests; government audits and investigations; and the application of the Federal Acquisition Regulation ("FAR") and individual agency supplement procurement regulations. Erin has also assisted with a variety of issues relating to internal investigations and other compliance matters associated with doing business with the federal government.



[Daniel Z. Herbst](#), Associate – Washington, D.C. · +1 202 414 9232 · [dherbst@reedsmith.com](mailto: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.



[Ed Hunter](#), Associate – London · +44 (0)20 3116 2997 · [ehunter@reedsmith.com](mailto:ehunter@reedsmith.com)

Ed joined Reed Smith as a trainee in February 2011 and joined the Employment Group on qualification in February 2013. Ed undertakes a wide range of contentious and non-contentious work, including advising on general employment matters such as terminations, bonus and restrictive covenant disputes and working time rights, as well as drafting contracts of employment and HR policies and procedures. Ed regularly advises on the employment aspects of corporate transactions, including business sales, share sales, private equity transactions and outsourcing matters. He also has experience working on large-scale projects such as global restructures and redundancy exercises.



[Lisa B. Kim](#), Associate – Los Angeles · +1 213 457 8043 · [lkim@reedsmith.com](mailto:lkim@reedsmith.com)

Lisa is a senior associate in the firm's Commercial Litigation Group. Lisa's practice focuses primarily on data privacy, security, and management, professional liability, and financial services. Lisa also has significant experience with landlord-tenant disputes, toxic tort matters, and general business disputes. Lisa defends businesses in data privacy class action litigation involving the Song-Beverly Credit Card Act, the Telephone Consumer Protection Act (TCPA), and other related statutes. Lisa also advises companies on compliance with various data privacy and security laws, including the TCPA, CAN-SPAM, the Video Privacy Protection Act (VPPA), California's Shine-the-Light law, and California's Do Not Track Disclosures. She writes and speaks regularly on new developments in California and federal law related to data privacy.



[Frederick H. Lah](#), Associate – New York · +1 212 549 0324 · [flah@reedsmith.com](mailto:flah@reedsmith.com)

Fred focuses his practice on data privacy, advertising, technology, and media. As a member of the Data Privacy, Security, and Management Group, Fred counsels clients on regulatory issues relating to data privacy such as data breach notification, telemarketing, e-mail marketing, mobile privacy, and children's privacy. He regularly advises companies on website privacy policies, terms of use, end user agreements, and data transfer and processing agreements. He has also assisted in the successful defense of a number of consumer privacy class actions. Fred is a Certified Information Privacy Professional ("CIPP"). He authored the note, "Are IP Addresses Personally Identifiable" for A Journal of Law and Policy for the Information Society. For the Advertising, Technology & Media Group, Fred represents clients on a wide range of legal issues surrounding advertising and marketing, including contests and sweepstakes, celebrity endorsement and talent agreements, social media marketing, sponsorship agreements, as well as trademark and copyright issues. His clients include advertising agencies, individual brands, financial institutions, professional sports teams, online service providers, and trade associations.



[Joelle E.K. Laszlo](#), Associate – Washington, D.C. · +1 202 414 9212 · [jlaszlo@reedsmith.com](mailto:jlaszlo@reedsmith.com)

Joelle is a member of the Global Regulatory Enforcement. Joelle's practice primarily involves assisting clients with issues related to federal and state contracts and grants, including the interpretation and applicability of: Federal Acquisition Regulation provisions and clauses, administrative and record-keeping requirements for contractors and grantees, and procurement and funding processes and procedures. Joelle has represented large and small business clients in bid protest actions before the Government Accountability Office, the U.S. Court of Federal Claims, the District of Columbia Contract Appeals Board, and other adjudicating bodies. She has also assisted with internal investigations related to government contract compliance, and responses to show cause letters and other notices of potential suspension and debarment.



[Kevin M. Madagan](#), Associate – Washington, D.C. · +1 202 414 9236 · [kmadagan@reedsmith.com](mailto: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.



[Bonnie M. Mangold](#), Associate – Pittsburgh · +1 412 288 5264 · [bmangold@reedsmith.com](mailto:bmangold@reedsmith.com)

Bonnie is an associate in Reed Smith's Financial Industry Group, practicing in the area of Financial Services Litigation. During law school, Bonnie worked as a summer associate at the firm and as a law clerk at Scottsdale Healthcare in the areas of Compliance and Risk Management.



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



[Alexandra A. Nelson](#), Associate – London · +44 (0)20 3116 3485 · [anelson@reedsmith.com](mailto:anelson@reedsmith.com)

Alexandra joined Reed Smith in 2007 when Richards Butler combined with the firm. She is a member of the Corporate Group.



[Jennifer Pike](#), Associate – Washington, D.C. · +1 202 414 9218 · [jpikse@reedsmith.com](mailto:jpikse@reedsmith.com)

Jennifer is a member of the Life Sciences Health Industry Group, practicing in the area of health care law. Her practice focuses on health care regulatory, compliance and enforcement matters, with a specific focus on entities regulated by the FDA. She counsels clients on regulatory and transactional issues related to biologic, pharmaceutical and medical device products in a variety of areas, including product marketing and clinical testing. In addition, she counsels clients on health information privacy and security compliance (HIPAA and state law), fraud and abuse compliance, Medicare reimbursement, and health care licensing issues..



[Meredith D. Pikser](#), Associate – New York · +1 212 521 5432 · [mpikser@reedsmith.com](mailto: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.



[Sachin Premnath](#), Associate – London · +44 (0)20 3116 3531 · [spremnath@reedsmith.com](mailto:spremnath@reedsmith.com)

Sachin is a senior associate in the Media & Technology Group. He specializes in advising clients on digital content licensing and distribution issues, software licensing, data protection, and related matters regarding the protection and exploitation of intellectual property rights on digital media networks and platforms. In particular, he has experience and expertise in digital music licensing, and structuring and negotiating commercial arrangements involving online music services, record labels, music publishers, collection societies and users.



[Jillian W. Riley](#), Associate – Pittsburgh · +1 412 288 3521 · [jwriley@reedsmith.com](mailto:jwriley@reedsmith.com)

Jillian joined Reed Smith as an associate in the Life Sciences Health Industry Group in 2013. She brought with her more than two years of experience with the U.S. Food and Drug Administration, Office of the Chief Counsel, where she served as Assistant Chief Counsel for Enforcement. Jillian's background includes pursuing enforcement actions from initiation through settlement or judgment against manufacturers of adulterated and misbranded drugs, medical devices, dietary supplements, tobacco, and various kinds of foods. This included personally negotiating many consent decrees on behalf of the agency.



[David A. Scharfstein](#), Associate – New York · +1 212 549 0296 · [dscharfstein@reedsmith.com](mailto:dscharfstein@reedsmith.com)

David is an associate in the complex commercial litigation group at Reed Smith LLP. He is an experienced litigator who handles a wide variety of commercial disputes, with a particular interest in trademark litigation and false advertising claims.



[Dr. Alin Seegel](#), Associate – Munich · +49 (0)89 20304 158 · [aseegel@reedsmith.com](mailto:aseegel@reedsmith.com)

Alin is an associate in the European Corporate Group in Munich and part of the Media & Technology Team. Alin has broad expertise covering contentious and non-contentious matters of IT law, in particular in the field of IT-outsourcing, negotiating and drafting of IT-agreements, data protection as well as in matters regarding IT-litigation and e-commerce. She also advises clients in cases relating to insolvency law issues.



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



[Jennifer M. Westhoff](#), Associate – Century City · +1 310 734 5261 · [jwesthoff@reedsmith.com](mailto:jwesthoff@reedsmith.com)

Jennifer is a member of Reed Smith's Corporate and Securities Group where she specializes in representing Entertainment clients. Jennifer has participated in multi-million dollar financing deals for production companies and individual television and film productions, film and television development and production agreements, purchases of record companies and groups of compositions, video game production agreements, and the purchase of films for distribution.

## — 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](http://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](http://www.facebook.com))

**Fast Pitch!** – A social network for business networking professionals to market their business, press, blogs, events and networks. ([www.fastpitchnetworking.com](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.slide.com))

**TypePad** – A blogging service for professionals and small businesses. TypePad hosts many popular blogs and small business websites. ([www.typepad.com](http://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](http://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](http://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](http://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](http://www.flickr.com))

**Photobasket** – An online storage site for users’ photos. ([photobasket.co.cc](http://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](http://photobucket.com))

**Picasa** – A free software download from Google that helps users organize, edit, and share photos. ([picasa.google.com](http://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](http://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](http://www.smugmug.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](http://www.twitxr.com))

**Zoomr** – A social utility for friends, family and co-workers who want to communicate securely through both photos and text messages in real-time. ([www.zoomr.com](http://www.zoomr.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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.live365.com))

**Justin.tv** – An online community for people to broadcast, watch and interact around live video. ([www.justin.tv](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.avvo.com))

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

**Concep** – An interactive email marketing platform. It allows users to create digital email campaigns and view statistics on readership. ([www.conceptglobal.com](http://www.conceptglobal.com))

**Constant Contact** – A site that helps organizations create professional-looking email newsletters and online surveys. ([www.constantcontact.com](http://www.constantcontact.com))

**Eventful** – An events website that enables its community of users to discover, promote, share and create events. ([www.eventful.com](http://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](http://www.google.com/alerts))

**Google Docs** – A web-based word processor and spreadsheet, which allows users to share and collaborate online. ([docs.google.com](http://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](http://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](http://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](http://www.readnotify.com))

**Sensidea** – A digital media consultancy and products company that helps clients deliver innovative digital strategies, products, and solutions. ([www.sensidea.com](http://www.sensidea.com))

**SurveyMonkey** – A tool to create and publish custom surveys, and then view results graphically and in real time. ([www.surveymonkey.com](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.mixx.com))

**My Yahoo!** – A customizable web page with news, stock quotes, weather, and many other features. ([my.yahoo.com](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://www.everyzing.com))

**Google Search** – A search engine that allows users to seek out content on the web. ([www.google.com](http://www.google.com))

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

**Yahoo! Search** – A web search engine that assists users in finding what they are looking for. ([search.yahoo.com](http://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](http://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](http://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](http://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](http://www.jott.com))

**Jumbuck** – A provider of community messaging applications to wireless carriers. ([www.jumbuck.com](http://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](http://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](http://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](http://www.aim.com))

**Go To Meeting** – A web conferencing software that allows users to work with anyone, anywhere, in online meetings. ([www.gotomeeting.com](http://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/](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](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](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, 2012.
- 15 State of the Media: The Social Media Report 2012, Nielsen, (2012)
- 16 Ring the Bells: More Smartphone in Students' Hands Ahead of Back-to-School Season, <http://www.nielsen.com/us/en/newswire/2013/ring-the-bells-more-smartphones-in-students-hands-ahead-of-back.html> (Oct. 29, 2013).
- 17 See, "Web Ad Spend Outstrips TV for First Time," *The Times*, Sept. 30, 2009.
- 18 "Social, Video Sites Will See Big Boosts in US Advertiser Spending," eMarketers (Oct. 15, 2013) (<http://www.emarketer.com/Article/Social-Video-Sites-Will-See-Big-Boosts-US-Advertiser-Spending/1010300>).
- 19 "B2Cs, B2Bs See Digital, Social Ad Spend Rising, as Traditional Stalls," eMarketers (Oct. 3, 2013) (<http://www.emarketer.com/Article/B2Cs-B2Bs-See-Digital-Social-Ad-Spend-Rising-Traditional-Stalls/1010270>).
- 20 <http://www.the-connection.com/social-media-reshaping-customer-care/>
- 21 <https://www.facebook.com/legal/terms>; <http://about.pinterest.com/terms/>; [http://www.tumblr.com/policy/en/terms\\_of\\_service](http://www.tumblr.com/policy/en/terms_of_service);
- 22 <http://www.youtube.com/t/terms>, and <https://twitter.com/tos>.
- 23 *Id.*
- 24 [https://www.facebook.com/page\\_guidelines.php](https://www.facebook.com/page_guidelines.php)
- 25 <https://support.twitter.com/articles/18366-impersonation-policy#>; <https://en.help.pinterest.com/entries/21134891-Pinterest-s-impersonation-policy>.
- 26 <http://help.instagram.com/464700830247492>
- 27 <http://support.twitter.com/articles/68877-guidelines-for-contests-on-twitter#>
- 28 [https://www.facebook.com/page\\_guidelines.php](https://www.facebook.com/page_guidelines.php)
- 29 [https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851577\\_158705844322839\\_2031667568\\_n.pdf](https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851577_158705844322839_2031667568_n.pdf)
- 30 <https://support.twitter.com/articles/68877-guidelines-for-contests-on-twitter#>; <http://business.pinterest.com/brand-guidelines/>
- 31 <https://doritocrashthesuperbowl.thismoment.com/>
- 32 <http://www.folgerscoffee.com/folgers-jingle/>
- 33 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.
- 34 N.Y. G.B.L. § 369-e and F.L. Stat. § 849.094.
- 35 *Id.*
- 36 R.I. Stat. Ch. 11-50, *et seq.*
- 37 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.
- 38 Nick Bilton, "Disruptions: Celebrities' Product Plugs on Social Media Draw Scrutiny," [http://bits.blogs.nytimes.com/2013/06/09/disruptions-celebrities-product-plugs-on-social-media-draw-scrutiny/?\\_r=0](http://bits.blogs.nytimes.com/2013/06/09/disruptions-celebrities-product-plugs-on-social-media-draw-scrutiny/?_r=0), June 9, 2013.
- 39 Michael Luca and Georgios Zervas, "Fake It Til You Make It: Reputation, Competition, and Yelp Review Fraud," (Sept. 24, 2013). <http://officialblog.yelp.com/2013/05/how-yelp-protects-consumers-from-fake-reviews.html>
- 40 "A.G. Schneiderman Announces Agreement With 19 Companies To Stop Writing Fake Online Reviews And Pay More Than \$350,000 In Fines," <http://www.ag.ny.gov/press-release/ag-schneiderman-announces-agreement-19-companies-stop-writing-fake-online-reviews-and>
- 41 16 CFR Part 255.

- 42 16 CFR § 255.1(d).
- 43 .com Disclosures: How to Make Effective Disclosures in Digital Advertising, Federal Trade Commission (Mar. 2013).
- 44 Paige Cooperstein, "Native Advertising: How It Works at the Huffington Post," <http://www.pbs.org/mediashift/2013/10/native-advertising-how-it-works-at-the-huffington-post/>, October 8, 2013.
- 45 Charlie Warzel, "The Real Problem With The Atlantic's Sponsored Post: Debacle proves that above all else, native ads need to feel native," <http://www.adweek.com/news/technology/real-problem-atlantics-sponsored-post-146553>, January 15, 2013.
- 46 <http://advertising.theatlantic.com/>
- 47 <http://fastlane.gmblogs.com>
- 48 <http://fastlane.gmblogs.com/about.html>
- 49 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.
- 50 <http://about.americanexpress.com/sm/>
- 51 <http://www.godaddy.com/socialmedia/social-media.aspx>
- 52 <http://www.fritolay.com/about-us/press-release-20130507a.html>
- 53 *Doctor's Associates Inc. v. QIP Holders LLC*, 82 U.S.P.Q.2d (BNA) 1603 (D. Conn. April 18, 2007).
- 54 Joseph Lewczak, "Quiznos/Subway Settlement Poses Threat to Future UGC Promos," *PROMO* Magazine, March 23, 2010.
- 55 *Seaton v. TripAdvisor LLC*, Opinion, No. 12-6122 (6th Cir. Aug. 28, 2013), available at <http://www.courthousenews.com/2013/09/03/tripad.pdf>
- 56 Christina Brinkley, "More Brands Want You to Model Their Clothes," *Wall Street Journal* (May 15, 2013) (<http://online.wsj.com/news/articles/SB10001424127887324216004578483094260521704>).
- 57 *Agence France Presse v. Morel*, Judgment, No. 10-cv-02730 (S.D.N.Y. Dec. 10, 2013).
- 58 *Eiselein v. Buzzfeed, Inc.*, Complaint, No. 1:13-cv-03910 (S.D.N.Y. Jun. 7, 2013).
- 59 Bundesgerichtshofentscheidung dated Nov. 12, 2009 (AZ I ZR 166/07, [www.marions.kuchbuch.de](http://www.marions.kuchbuch.de)).
- 60 BGH order for reference dated Mai 16, 2013 (AZ I ZR 46/12 – framing).
- 61 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.
- 62 The authors wish to acknowledge the contributions of John L. Hines and Janice D. Kubow to the content of this chapter.
- 63 See, Cass R. Sunstein, "On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done," (Farrar, Straus, and Giroux 2009).
- 64 The Impact of the Class Action Fairness Act of 2005 on the Federal Courts.
- 65 15 U.S.C. § 45.
- 66 15 U.S.C. § 1125(a).
- 67 15 U.S.C. § 45.
- 68 Available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>
- 69 *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).
- 70 *Int'l Harvester Co.*, 104 FTC 949 1058 (1984).
- 71 *Sandoz Pharmaceuticals v. Richardson-Vicks*, 902 F.2d 222, 228 (3d Cir. 1990).
- 72 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).
- 73 *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).
- 74 *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.").
- 75 *U.S. Healthcare*, 898 F.2d at 921 (3d Cir. 1990) (quoting 2 J. McCarthy, *Trademarks and Unfair Competition* § 27:713 (2d Ed. 1984)).
- 76 See, e.g., *Bruno v. Quten Research Inst., LLC*, 280 F.R.D. 524 (C.D. Cal. 2011) (class-action lawsuit instituted after NAD finding that advertiser possessed insufficient support for its claim that its liquid dietary supplement was absorbed six times "better" than competing products).
- 77 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).
- 78 FTC Guides, at 53125, n.11.
- 79 FTC Guides, § 255.0.
- 80 FTC Guides, at 8.
- 81 15 U.S.C. § 45.
- 82 FTC Guides, § 255.1(d).
- 83 FTC Guides, at 38-39.
- 84 FTC Guides, § 255.1(d).
- 85 FTC Guides, at 42.
- 86 *Id.*
- 87 FTC Guides, at 15.
- 88 *Id.*
- 89 FTC Guides, at 39.

- 90 FTC Guides, at 40, 42.
- 91 Federal Trade Commission, *.com Disclosures*, available at <http://www.business.ftc.gov/documents/bus41-dot-com-disclosures-information-about-online-advertising>.
- 92 *Id.* at p. iii
- 93 *Id.* at A-18.
- 94 See *Spencer v. Sensa Products, LLC*, Index No. BC519632 (Cal. Super. Ct. 2013).
- 95 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).
- 96 The CAP Code can be found on CAP’s website at <http://www.cap.org.uk>.
- 97 See: <http://www.asa.org.uk/News-resources/Hot-Topics/-/media/Files/ASA/Hot%20Topics/Charity%20advertising%20-%20Hot%20topic.ashx>
- 98 Restatement, Second, Torts § 558.
- 99 *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 Blogger.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).
- 100 *E.g., Stratton Oakmont v. Prodigy*, 1995 WL 323710, at \*3 (N.Y. Sup. Ct., May 24, 1995) (Unreported).
- 101 *E.g., Cubby v. Compuserve*, 776 F.Supp. 135 (S.D.N.Y. 1991).
- 102 47 U.S.C. § 230 (“CDA”).
- 103 47 U.S.C. § 230(c)(1).
- 104 47 U.S.C. § 230(f)(3).
- 105 474 F.Supp. 2d 843 (W.D. Tex. 2007).
- 106 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.
- 107 474 F.Supp.2d at 849.
- 108 *Black v. Google, Inc.*, 457 F. App’x 622, 623 (9th Cir. 2011) (“The district court properly dismissed plaintiffs’ action as precluded by [the CDA] because plaintiffs seek to impose liability on Google for content created by a third party.”); *Getachew v. Google, Inc.*, 491 F. App’x 923, 925 (10th Cir. 2012) (“Under [the CDA], Google cannot be held liable for search results that yield content created by a third party”).
- 109 2009 WL 3240365, No. 102578/09 (N.Y. Sup. Sept. 15, 2009).
- 110 2009 WL 3240325, at \*1.
- 111 2009 WL 3240365, at \*1 (*citing Blumenthal v. Drudge*, 992 F.Supp. 44, 52 (D.D.C. 1998)).
- 112 478 F.3d 413 (1st Cir. 2007).
- 113 *Id.* at 421.
- 114 521 F.3d 1157 (9th Cir. 2008) (*en banc*).
- 115 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).
- 116 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).
- 117 *Shiamilli v. Real Estate Grp. of New York, Inc.*, 17 N.Y.3d 281, 290, 952 N.E.2d 1011, 1018 (2011).
- 118 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).
- 119 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).
- 120 47 U.S.C. § 230(e)(2).
- 121 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”).
- 122 488 F.3d 1102 (9th Cir.), *cert. denied*, 128 S.Ct. 709 (2007).
- 123 *Id.* at 1118-19.
- 124 540 F.Supp.2d 299-304. *Accord, Atlantic Recording Corporation v. Project Playlist*, 603 F.Supp.2d 690 (S.D.N.Y. 2009) (“if Congress wanted the phrase ‘any law pertaining to intellectual property’ to actually mean ‘any federal law pertaining to intellectual property,’ it knew how to make that clear, but chose not to”); *Universal Commc’n Sys., Inc. v. Lycos*, 478 F.3d 413, 422-23 (1st Cir. 2007) (stating in dicta that “[c]laims based on intellectual property laws are not subject to Section 230 immunity.”); *Parisi v. Sinclair*, 774 F. Supp. 2d 310, 317-18 (D.D.C. 2011) (stating in dicta that the court is “not inclined to extend the scope of the CDA immunity as far as the Ninth Circuit”).
- 125 O’Grady v. Superior Court (Apple Computer, Inc.), 39 Cal.App.4th 1423 (Sixth Dist. 2006).
- 126 See, *e.g., Too Much Media, LLC v. Hale*, 2010 WL 1609274, A-0964-09 (N.J. Super. A.D., April 22, 2010) (rejecting defendant’s assertion of the reporter’s privilege with respect to his pornography blog because, among other reasons, 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.”)
- 127 558 U.S. 310, 352, 130 S. Ct. 876, 905-06, 175 L. Ed. 2d 753 (2010).
- 128 2014 WL 185376 (Jan. 17, 2014).
- 129 175 F.3d 848 (10th Cir. 1999) (affirming dismissal of claims directed to credit ratings based on First Amendment).
- 130 2003 WL 21464568, No. CIV-02-1457-M (W.D. Ok., May 27, 2003).
- 131 2011 WL 5079526 (N.D. Cal. Oct. 26, 2011)
- 132 *Id.* at \*6.
- 133 *Id.* at \*7.
- 134 *Id.*
- 135 *Id.* at \*8.
- 136 *Cairns v Modi* ([2012] EWCA Civ 1382).
- 137 *McAlpine v Bercow* ([2013] EWHC 1342 (QB))
- 138 **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.**
- 139 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.
- 140 *Bundesgerichtshof* [German Federal Court of Justice], GRUR 2004, p. 860 – Internet auction I.
- 141 *Bundesgerichtshof* [German Federal Court of Justice], GRUR 2007, p. 708 – Internet auction II.
- 142 See, for example, *Bundesgerichtshof* [German Federal Court of Justice], GRUR 1999, p. 418.
- 143 17 U.S.C. § 102 (a).
- 144 S. 1 (1) UK Copyright Designs and Patents Act.
- 145 § 2 (2) German Copyright Act.
- 146 Such as in § 51 German Copyright Act.
- 147 The author wishes to acknowledge the contributions of Rachel A. Rubin to the content of this chapter.
- 148 Twitter Terms of Service (effective June 25, 2012), <https://twitter.com/tos?PHPSESSID=57a411f70b1964a2bc78b82638ba1843>
- 149 Facebook Statement of Rights and Responsibilities (last revised Nov. 15, 2013), <https://www.facebook.com/legal/terms>
- 150 Instagram Terms of Use (effective January 19, 2013), <http://instagram.com/legal/terms/#>
- 151 YouTube Terms of Service (June 9, 2010), <https://www.youtube.com/static?template=terms>
- 152 Evelyn M. Rusli, *Facebook Buys Instagram for \$1 Billion*, N.Y. TIMES DEALBOOK BLOG (Apr. 9, 2012), [http://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/?\\_php=true&\\_type=blogs&\\_r=0](http://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/?_php=true&_type=blogs&_r=0)
- 153 Erin Geiger Smith, *News outlets improperly used photos posted to Twitter: judge*, REUTERS (Jan. 15, 2013), <http://www.reuters.com/article/2013/01/15/us-socialmedia-copyright-ruling-idUSBRE90E11P20130115>
- 154 Joseph Ax, *Photographer wins \$1.2 million from companies that took pictures off Twitter*, REUTERS (Nov. 22, 2013), <http://www.reuters.com/article/2013/11/22/us-media-copyright-twitter-idUSBRE9AL16F20131122>
- 155 17 U.S.C. § 1201 (2013)
- 156 Online service providers include any company, organization or group that provides an online service, including social media sites.
- 157 17 U.S.C. § 512(c)(3)(A)(i-vi) (2013)
- 158 *Id.*
- 159 <https://www.facebook.com/help/contact/208282075858952>
- 160 <https://support.twitter.com/forms/dmca>
- 161 <http://www.youtube.com/yt/copyright/copyright-complaint.html>
- 162 17 U.S.C. § 512(c)(3)(A)(i-vi) (2013)
- 163 *Perfect 10, Inc. v. Amazon.com, Inc.*, 487 F.3d 701 (9th Cir. 2007)
- 164 *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005)
- 165 *Ashcroft v. Iqbal*, 556 U.S. 662 (2009)
- 166 *Elf Man, LLC. v. Cariveau*, No. C13-0507 RSL, (W.D. Wash. Jan. 17, 2014)
- 167 *Id.*
- 168 Facebook Platform Policy (last revised Aug. 20, 2013), <https://developers.facebook.com/policy/>
- 169 Twitter Developer Rules of the Road (last updated Jul. 2, 2013), <https://dev.twitter.com/terms/api-terms>
- 170 Federal Trade Commission, *16 CFR Part 255—Guides Concerning the Use of Endorsements and Testimonials in Advertising*, available at <http://ftc.gov/os/2009/10/091005revisedendorsementguides.pdf>
- 171 The authors wish to acknowledge the contributions of Amy S. Mushahwar and Gregory J. Payor to the content of this chapter.
- 172 “Press Room,” available at: <https://newsroom.fb.com/Key-Facts>
- 173 Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers,” available at: <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. (Mar. 26, 2012) (hereinafter “FTC Final Report”); Department of Commerce, “Consumer Data in a Networked

- World" available at:  
<http://www.google.com/url?sa=t&rc=1&q=&esc=s&frm=1&source=web&cd=1&ved=0CCcQIAA&url=http%3A%2F%2Fwww.commerce.gov%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2F2012%2FFebruary%2Fprivacy-final.pdf>  
 &ei=juHIUrrGIMrNsQSV\_oCOBA&usq=AFQjCNGST\_wR3Vz0bETcA2ZcsOOIW5JruQ&sig2=UTGI6r2EUlr9astubNj-g&bvm=bv.59930103.d.cWc (Feb. 23, 2012)
- 174 John Lister, "Most Departing Employees Steal Company Data," Tech.Blorge (Feb. 23, 2009) available at:  
<http://tech.blorge.com/Structure:%202009/02/23/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).
- 175 Working Document 02/2013 providing guidance on obtaining consent for cookies- WP 208 (02.10.2013)" available at: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion\\_recommendation/files/2013/wp208\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion_recommendation/files/2013/wp208_en.pdf)
- 176 For example, the Gramm-Leach-Bliley Act requires certain types of companies (financial institutions, insurance companies and brokerage companies) to maintain privacy policies. In addition, the California Online Privacy Protection Act requires a website or online service operator to conspicuously post its privacy policy on the website or make it available through the online service. See Cal. Bus. & Prof. Code § 22575. Effective January 1, 2015, website and online service providers will have to allow minors erase their own posts on social media. See Cal. Bus. & Prof. Code § 22580.
- 177 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.
- 178 Catharine Smith, "Facebook, FTC Reach Settlement Over Alleged Privacy Violations," Huffington Post (Nov. 29, 2011) available at:  
[http://www.huffingtonpost.com/2011/11/29/facebook-ftc-reach-settle\\_n\\_1118996.html](http://www.huffingtonpost.com/2011/11/29/facebook-ftc-reach-settle_n_1118996.html)
- 179 Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," Press Release (Nov. 29, 2011) available at: <http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>
- 180 Federal Trade Commission, "FTC Approves Final Settlement With Facebook," Press Release (Aug. 10, 2012) available at: <http://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>
- 181 Center for Digital Democracy, "EPIC & CDD ask Facebook's Mark Zuckerberg to withdraw proposed changes weakening user rights and expanding data collection," (Nov. 26, 2012), available at: <http://www.centerfordigitaldemocracy.org/epic-cdd-ask-facebooks-mark-zuckerberg-withdraw-proposed-changes-weakening-user-rights-and-expanding>
- 182 "FTC Looking Into Facebook's Proposed Privacy Policy Changes," Huffington Post (Sept. 12, 2013), available at:  
[http://www.huffingtonpost.com/2013/09/12/ftc-looking-into-proposed\\_n\\_3915645.html](http://www.huffingtonpost.com/2013/09/12/ftc-looking-into-proposed_n_3915645.html)
- 183 Facebook, Inc., "Thanks For Your Feedback," (Nov. 15, 2013), available at: <https://www.facebook.com/notes/facebook-site-governance/thanks-for-your-feedback/10153503594325301>
- 184 Heather Kelly, "Facebook changes privacy settings for teens," CNN (Oct. 31, 2013), available at: <http://www.cnn.com/2013/10/16/tech/social-media/facebook-teens-privacy/>
- 185 [http://ec.europa.eu/justice\\_home/fsj/privacy/news/docs/pr\\_28\\_01\\_10\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_28_01_10_en.pdf) .
- 186 "Google Wins Louis Vuitton Trademark Case" 23.03.2010 available at: : <http://www.theguardian.com/media/2010/mar/23/google-louis-vuitton-search-ads>
- 187 "Opinion of Advocate General Poaires Maduro in the Joined Cases C-236/08-C-238/08" available at:  
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=73281&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=288109> ; also See "Judgment of the Court (Grand Chamber) of 23 March 2010 (reference for a preliminary ruling from the Cour de cassation - France) - Google France, Google, Inc. v Louis Vuitton Malletier (C-236/08), Viaticum SA, Luteciel SARL (C-237/08), Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08)," available at :  
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=288109> .
- 188 "Opinion of Advocate General Jaaskinen delivered on 25 July 2013 in the Case of C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD),"available at:  
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=292528> ; also See: "ECJ Press Release on Advocate General's Opinion in Case C-131/12 dated 25 June 2013,"available at :  
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf>
- 189 "Google not obliged to delete data, rules EU lawyer" 25.06.2013 available at: <http://www.bbc.co.uk/news/technology-23044809>
- 190 "Judgement of the Honourable Mr Justice Tugendhat of Vidal -Hall & Ors v Google Inc [2014] EWHC 13 (QB) (16 January 2014)" available at:  
<http://www.bailii.org/ew/cases/EWHC/QB/2014/13.html>
- 191 "Google must face UK courts over claims of privacy breach of iPhone users" 16.01.2014 available at:  
<http://www.theguardian.com/technology/2014/jan/16/google-uk-courts-privacy-breach-iphone-safari>
- 192 "Google privacy policy slammed by EU data protection chiefs" available at: <http://www.theguardian.com/technology/2012/oct/16/google-privacy-policies-eu-data-protection>
- 193 "Google Fined for Illegally Collecting Personal Data" available at: [http://english.chosun.com/site/data/html\\_dir/2014/01/29/2014012901599.html](http://english.chosun.com/site/data/html_dir/2014/01/29/2014012901599.html)
- 194 "Google to be told by EU to unravel privacy policy" available at: <http://www.theguardian.com/technology/2012/oct/15/google-privacy-policy>
- 195 "The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc." 08.01.2014 available at: <http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-eur-monetary-penalty-to-google-inc/>
- 196 See Press Release "The AEPD sanctions Google for serious violation of the rights of the citizens" 19.12.2013 available at:  
[http://www.agpd.es/portalwebAGPD/revista\\_prensa/revista\\_prensa/2013/notas\\_prensa/common/diciembre/131219\\_PR\\_AEPD\\_PRI\\_POL\\_GOOGLE.pdf](http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/diciembre/131219_PR_AEPD_PRI_POL_GOOGLE.pdf) ; also see "Spain levies maximum fine over Google privacy policy" 20.12.2013 available at: <http://www.bbc.co.uk/news/technology-25461353>

- 197 See Press Release of European Parliament 21.10.2013 "Civil Liberties MEPs pave the way for stronger data protection in the EU" available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>
- 198 "Facebook loses friends as privacy campaign grows" 14.05.2010 available at: <http://www.theguardian.com/technology/2010/may/14/facebook-privacy-campaign-delete-account>
- 199 "Facebook could face €100,000 fine for holding data that users have deleted" 20.10.2011 available at: <http://www.theguardian.com/technology/2011/oct/20/facebook-fine-holding-data-deleted>
- 200 "Student group to take Facebook to task in Irish court " 04.12.2012 available at: <http://www.bbc.co.uk/news/technology-20592799>
- 201 "Facebook Ireland Audit Report- December 2011" available at: [http://dataprotection.ie/viewdoc.asp?m=&fn=/documents/Facebook\\_Report/final\\_report/report.pdf](http://dataprotection.ie/viewdoc.asp?m=&fn=/documents/Facebook_Report/final_report/report.pdf); also see "Irish privacy watchdog calls for Facebook changes" 21.12.2011 available at: <http://www.bbc.co.uk/news/technology-16289426>
- 202 "Facebook facial recognition software violates privacy laws, says Germany " 03.08.2011 available at: <http://www.theguardian.com/technology/2011/aug/03/facebook-facial-recognition-privacy-germany>
- 203 "German state fights Facebook over alleged privacy violations " 04.01.2013 available at: <http://www.theguardian.com/world/2013/jan/04/facebook-germany-data-protection>
- 204 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.")
- 205 Twitter, The Twitter Rules, <https://support.twitter.com/articles/18311#>
- 206 Twitter, How to report violations, <https://support.twitter.com/articles/15789-how-to-report-violations#>
- 207 Facebook Statement of Rights and Responsibilities, available at: <https://www.facebook.com/legal/terms> (last visited, Jan. 28, 2014).
- 208 *Id.* at § 5.8.
- 209 Instagram, Learn How to Address Abuse, available at: <http://help.instagram.com/527320407282978/> (last visited, Jan. 28, 2014).
- 210 Instagram, Community Guidelines, available at: <http://help.instagram.com/477434105621119> (last visited, Jan. 28, 2014).
- 211 Pinterest, Acceptable Use Policy, available at: <http://about.pinterest.com/use/> (last visited, Jan. 28, 2014).
- 212 *Id.*
- 213 Pinterest, Report objectionable or spammy content, comments or people, available at: <https://help.pinterest.com/entries/22163668-Report-objectionable-or-spammy-content-comments-or-people> (last visited, Jan. 28, 2014).
- 214 MySpace.com Terms of Use Agreement, last updated June 10, 2013, available at: <https://www.myspace.com/pages/terms> (last visited, Jan. 28, 2014).
- 215 *Id.* at §§ 8.2.
- 216 "Snapchat's expired snaps are not deleted, just hidden," The Guardian, available at: <http://www.theguardian.com/media-network/partner-zone-infosecurity/snapchat-photos-not-deleted-hidden>
- 217 Snapchat, How Snaps Are Stored and Deleted, available at: <http://blog.snapchat.com/post/50060403002/how-snaps-are-stored-and-deleted> (May 9, 2014).
- 218 Twitter, Twitter supports Do Not Track, available at: <https://support.twitter.com/articles/20169453-twitter-supports-do-not-track#> ("When you turn on DNT in your browser, we stop collecting the information that allows us to tailor suggestions based on your recent visits to websites that have integrated our buttons or widgets. We also stop collecting the information that allows us to tailor ads based on your visits to our ad partners' websites. Specifically, we stop collecting the unique browser cookie that links your browser to visits to these websites for tailoring suggestions or ads.") (last visited, Jan. 28, 2014).
- 219 Pinterest, What's this "Do Not Track" thing?, available at: <https://help.pinterest.com/entries/24996501-What-s-this-Do-Not-Track-thing-> (last visited, Jan. 28, 2014).
- 220 Office of the Privacy Commissioner of Canada, "WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities," available at: [http://www.priv.gc.ca/media/nr-c/2013/nr-c\\_130128\\_e.asp](http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp) (Jan. 28, 2013).
- 221 Federal Trade Commission, "Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books," <http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived> (Feb. 1, 2013).
- 222 See "Proposal for General Data Protection Regulation (the Regulation)" available at: <http://register.consilium.europa.eu/pdf/en/12/st05/st05853.en12.pdf>.
- 223 See " Proposal for Data Protection Directive (the Directive) covering law enforcement" available at: <http://register.consilium.europa.eu/pdf/en/12/st05/st05833.en12.pdf>.
- 224 "EU Panel Data Protection Regulation Vote Delayed Until Fall by Amendments" available at: [http://privacylaw.bna.com/pvrc/7060/split\\_display.adp?fedfid=32440623&vname=prabulallissues&jd=a0d9p0q1u4&split=0](http://privacylaw.bna.com/pvrc/7060/split_display.adp?fedfid=32440623&vname=prabulallissues&jd=a0d9p0q1u4&split=0)
- 225 *McKeogh v John Doe 1 & Ors* [2012] available at <http://www.baillii.org/ie/cases/I/EHC/2012/H95.html>
- 226 [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm)
- 227 Opinion 5/2009 on online social networking, p. 6.
- 228 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.
- 229 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*).
- 230 See "Social networking and online forums- when does the DPA apply?" available at: [http://www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/social-networking-and-online-forums-dpa-guidance.ashx](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/social-networking-and-online-forums-dpa-guidance.ashx)

- 231 See "ICO Privacy Notices Code of Practice" available at: [http://ico.org.uk/for\\_organisations/guidance\\_index/-/media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/PRIVACY\\_NOTICES\\_COP\\_FIN\\_AL.ashx](http://ico.org.uk/for_organisations/guidance_index/-/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FIN_AL.ashx)
- 232 "Making privacy notices meaningful" The Reporter (Calleja Consulting) July 2009.
- 233 Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," available at: <http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep> (Nov. 29, 2011).
- 234 Federal Trade Commission, "Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers," <http://www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about> (May 8, 2012).
- 235 Portions of this chapter first appeared in, and are reprinted with permission of, the *Privacy & Security Law Journal*.
- 236 "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.).
- 237 Drew Hendricks, "Facebook To Drop Sponsored Stories: What Does This Mean For Advertisers?," available at <http://www.forbes.com/sites/drewhendricks/2014/01/16/facebook-to-drop-sponsored-stories-what-does-this-mean-for-advertisers/> (Jan. 16, 2014).
- 238 David Kravets, "Judge Approves \$20M Facebook 'Sponsored Stories' Settlement," *Wired* (Aug. 26, 2013) available at: <http://www.wired.com/threatlevel/2013/08/judge-approves-20-million-facebook-sponsored-stories-settlement/>
- 239 IAB, Self-Regulatory Principles for Online Behavioral Advertising, available at [http://www.iab.net/insights\\_research/public\\_policy/behavioral-advertisingprinciples](http://www.iab.net/insights_research/public_policy/behavioral-advertisingprinciples)
- 240 Council of Better Business Bureaus, The National Partner Program, available at: <http://www.bbb.org/council/the-national-partner-program/national-advertising-review-services/accountability-program/case-decisions/> (last visited, Jan. 28, 2014).
- 241 See Article 29 Working Party "Opinion 2/2010 on online behavioural advertising" available at: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf) ; also see Article 29 Working Party "Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising" available at: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf) .
- 242 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*).
- 243 See "EASA Best Practice Recommendations For Online Behavioural Advertising" available at: [http://www.easaalliance.org/binarydata.aspx?type=doc/EASA\\_BPR\\_OBA\\_12\\_APRIL\\_2011\\_CLEAN.pdf/download](http://www.easaalliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download)
- 245 See CAP "Rules For Organisations Conducting Online Behavioural Advertising" available at: <http://www.cap.org.uk/News-reports/Media-Centre/2012/-/media/Files/CAP/Misc/New%20Online%20Behavioural%20Advertising%20rules.ashx>
- 246 Yelp, "Deals, Gift Certificates, and Check-in Offers," <http://www.yelp.com/advertise/national/offer>
- 247 Federal Trade Commission, "FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures," Press Release, available at: <http://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy> (Feb. 1, 2013).
- 248 State of California Department of Justice, "Attorney General Kamala D. Harris Issues Guidance on How Mobile Apps Can Better Protect Consumer Privacy," available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-guidance-how-mobile-apps-can-better> (Jan. 10, 2013).
- 249 Federal Trade Commission, "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers," available at: <http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived> (Dec. 5, 2013).
- 250 "The NSA Files" available at <http://www.theguardian.com/world/the-nsa-files>
- 251 "LIBE Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))" available at: <http://www.statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf>
- 252 *Hays v. Ions*, EWHC (Ch), No. 745, 4/16/2008. available at <http://www.bailii.org/ew/cases/EWHC/Ch/2008/745.html> ; also see *Whitmar Publications Ltd. v. Gamage*, EWHC (Ch), No. 1881, 7/4/2013 available at: <http://www.bailii.org/ew/cases/EWHC/Ch/2013/1881.html>
- 253 See Joseph Menn, "Social networks scan for sexual predators, with uneven results," *Chicago Tribune*, dated July 12, 2012, available at [http://articles.chicagotribune.com/2012-07-12/business/sns-rt-usa-internetpredators12e8iady1-20120711\\_1\\_predators-smartphone-app-facebook](http://articles.chicagotribune.com/2012-07-12/business/sns-rt-usa-internetpredators12e8iady1-20120711_1_predators-smartphone-app-facebook) ; see also Justin P. Murphy and Adrian Fontecilla, "Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues," 19 *Rich. J.L. & Tech.* 11, 7 (2013).
- 254 Emma W. Sholl, "Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence" , 16 *Tul. J. Tech. & Intell. Prop.* 207, 223 (Fall 2013), citing *Romano v. Steelcase Inc.*, 30 *Misc.3d.* 426, 432-33 (2010).
- 255 John Browning, "It's Complicated: How to Walk the Fine Ethical Line in the Age of Social Media," 76 *Tex. Bar Journal* 959, 961 (2013).
- 256 Tariq Remtulla, "Facebook Not So Private? Ontario Court Finds Facebook Profile Discoverable," 14 No. 4 *Cyberspace Law* 17 (May 2009).
- 257 *Pre-paid Legal Services, Inc. v. Cahill*, 924 F.Supp.2d 1281, 1292-93 (E.D. Okla. 2013).
- 258 IT-Lex Technology Law, "NLRB Looks At Retaliatory Firings Based On Facebook Posts," <http://it-lex.org/nlrp-looks-at-retaliatory-firings-based-on-facebook-posts/> (Apr. 30, 2013).
- 259 Margaret DiBianca, "Warnings Against LinkedIn Recommendations: Justified or Propaganda?" 14 No. 9 *Del. Emp. L. Letter* 2 (Sept. 2009).
- 260 See Harry Haydon *The Sun* dated 05 Jul 2009, available at <http://www.thesun.co.uk/sol/homepage/news/2517719/M16-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).

- 261 See generally *Leser v. Peñido*, 96 A.D.3d 578 (2012); *Internet Solutions Corp. v. Marshall*, 611 F.3d 1368 (11th Cir. 2010); *Doe I, et al. v. Individuals*, 561 F.Supp.2d 249 (D. Conn. 2008).
- 262 "Service of Process Through Facebook" 03.10.2011 available at: <http://www.lexisnexis.com/legalnewsroom/international-law/b/international-law-blog/archive/2011/03/10/service-of-process-through-facebook.aspx>
- 263 MKM Capital Property Limited v Corbo and Poyser, No. SC 608 of 2008
- 264 *Axe Market Gardens v Craig Axe* CIV: 2008-485-2676
- 265 *Knott v. Sutherland* (Feb. 5, 2009) Edmonton 0803 002267 (Alta.Q.B.M.)
- 266 "Service via Twitter – the UK courts embrace technology" The Reporter (Calleja Consulting) November 2009; also see "Court order served over twitter" available at <http://news.bbc.co.uk/1/hi/8285954.stm>
- 267 AKO Capital and AKO Master Fund against former broker TFS Derivatives; also see "Legal claims can be served via Facebook, High Court judge rules" 21.02.2012 available at: <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/9095489/Legal-claims-can-be-served-via-Facebook-High-Court-judge-rules.html>
- 268 Federal Trade Commission, "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule," available at: <http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over> (Dec. 19, 2012).
- 269 "Warsaw Declaration on the application of society" available at: <https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf> .
- 270 "Digital Agenda: children using social networks at a younger age; many unaware of basic privacy risks, says survey" 18.04.2011 available at: [http://europa.eu/rapid/press-release\\_IP-11-479\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-11-479_en.htm?locale=en)
- 271 "Digital pictures and facial recognition in our digital life: trends and challenges for tomorrow" 03.2013 available at: [http://www.cnil.fr/fileadmin/documents/en/LettreIP4\\_en\\_def.pdf](http://www.cnil.fr/fileadmin/documents/en/LettreIP4_en_def.pdf) ; also see "First Issue of CNIL IP Reports – Privacy Towards 2020" available at <http://www.cnil.fr/english/news-and-events/news/article/first-issue-of-cnil-ip-reports-privacy-towards-2020-42-experts-share-their-visions-of-the/>
- 272 [http://ec.europa.eu/information\\_society/activities/social\\_networking/eu\\_action/selfreg/index\\_en.htm](http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm)
- 273 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.
- 274 For example, taking steps to ensure that private profiles of users registered as under 18 are not searchable.
- 275 [http://ec.europa.eu/cyprus/news/20100209\\_safer\\_internet\\_en.htm](http://ec.europa.eu/cyprus/news/20100209_safer_internet_en.htm)
- 276 See "Self-regulation for a Better Internet for Kids" available at: <http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids>
- 277 See "Safer Internet Day events in Brussels: Neelie Kroes to hand out prizes for Best Online Content for Kids " 12.05.2013 available at: <http://ec.europa.eu/digital-agenda/en/news/safer-internet-day-events-brussels-neelie-kroes-hand-out-prizes-best-online-content-kids>
- 278 See "ICO- Personal Information Online- Code of Practice" available at: [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/online/personal\\_information\\_online](http://ico.org.uk/for_organisations/data_protection/topic_guides/online/personal_information_online)
- 279 See <http://www.getsafeonline.org/businesses/data-protection-act/> ; <http://www.thinkuknow.co.uk/>
- 280 See "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998" available at: [http://ico.org.uk/enforcement/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/ico\\_guidance\\_on\\_monetary\\_penalties.pdf](http://ico.org.uk/enforcement/~media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf)
- 281 See sections 4, 55, 55A and 55B of the Data Protection Act 1998 (as amended).
- 282 Christopher Niebel v The Information Commissioner (EA/2012/2060) available at: <http://www.informationtribunal.gov.uk/DBFiles/Decision/i1106/Niebel.%20Christopher%20EA.2012.0260.pdf> ; also see *Scottish Borders Council v The Information Commissioner* (EA/2012/0212) available at: [http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20\(210813\)%20Preliminary%20Decision.pdf](http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20(210813)%20Preliminary%20Decision.pdf)
- 283 Facebook, "Information for Law Enforcement Authorities"; Google, "Transparency Report," available at: <http://www.google.com/transparencyreport/userdatarequests/legalprocess/> ; Twitter, "Guidelines for Law Enforcement," available at: <http://support.twitter.com/articles/41949-guidelines-for-law-enforcement#>
- 284 Russ Buettner, "Judge Orders Twitter to Release Protester's Messages," available at: <https://www.facebook.com/safety/groups/law/guidelines/> ; New York Times: City Room (Jul. 2, 2012), available at: <http://cityroom.blogs.nytimes.com/2012/07/02/judge-orders-twitter-to-release-protesters-messages/>
- 285 Somini Sengupta, "Twitter Appeals to Protect Protestor's Tweets," New York Times: Bits (Jul. 19, 2012), available at: [http://bits.blogs.nytimes.com/2012/07/19/twitter-appeals-to-protect-protesters-tweets/?\\_php=true&\\_type=blogs&\\_r=0](http://bits.blogs.nytimes.com/2012/07/19/twitter-appeals-to-protect-protesters-tweets/?_php=true&_type=blogs&_r=0)
- 286 Russ Buettner, "A Brooklyn Protester Pleads Guilty After His Twitter Posts Sink His Case," New York Times (Dec. 12, 2012), available at: <http://www.nytimes.com/2012/12/13/nyregion/malcolm-harris-pleads-guilty-over-2011-march.html>
- 287 Jose Pagliery, "2 million Facebook, Gmail and Twitter passwords stolen in massive hack," CNN Money (Dec. 4, 2013), available at: <http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/>
- 288 Doug Gross, "Millions of accounts compromised in Snapchat hack," CNN (Jan. 2, 2014), available at: <http://www.cnn.com/2014/01/01/tech/social-media/snapchat-hack/>
- 289 Joel Schectman, "UPDATE: LinkedIn Confirms Security Breach," Wall Street Journal: Digits (Jun. 6, 2012), available at: <http://blogs.wsj.com/digits/2012/06/06/two-security-firms-say-they-verified-linkedin-breach/>
- 290 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, Nicolas Sauvage and Amber Spataro.

- 291 <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.
- 292 "Social networking and reputational risk in the workplace," Deloitte LLP 2009 Ethics & Workplace Survey results.
- 293 <http://www.marketwire.com/press-release/Proofpoint-Inc-1027877.html>.
- 294 <http://www.independent.co.uk/news/media/current-twitter-trends-sun-ceo-tweets-his-resignation-modern-haikus-1889534.html>.
- 295 <http://www.workforce.com/section/02/feature/26/66/08/#>.
- 296 Schedule 1(1) and Schedule 2(1) Data Protection Act 1998  
<http://www.statutelaw.gov.uk/legResults.aspx?LegType=All%20Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610>.
- 297 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](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf).
- 298 ACAS Code of Practice <http://www.acas.org.uk/index.aspx?articleid=2175>.
- 299 French Labor Code, articles L. 1221-6, L. 1221-8, L. 1221-9, L. 2323-32.
- 300 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.
- 301 The HALDE (*"Haute Autorité de Lutte contre les Discriminations et pour l'Égalité"*) 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>.
- 302 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.
- 303 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.
- 304 Such as the MEDEF (The Mouvement des Entreprises de France), employers' organization representing the French business leaders.
- 305 *"Charte réseaux sociaux, Internet, Vie Privée et Recrutement"*.
- 306 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).
- 307 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.
- 308 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.
- 309 See *Blakley v. Continental Airlines, Inc.* 751 A.2d 538 (N.J. 2000)
- 310 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.
- 311 See *Doe v. XYZ Corp.*, 887 A.2d. 1156 (N.J. Super. 2005).
- 312 16 CFR Part 255.
- 313 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](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf).
- 314 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>.
- 315 *Otomewo v Carphone Warehouse Ltd* ET/2330554/2011.
- 316 See for example, *Teggart v TeleTech UK Ltd* [2012] NIIT 00704\_11IT; *Gosden v Lifeline Project Ltd* ET/2802731/2009.
- 317 [http://www.theregister.co.uk/2008/10/23/sickie\\_woo](http://www.theregister.co.uk/2008/10/23/sickie_woo).
- 318 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.
- 319 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.
- 320 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."

- 321 "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").
- 322 <http://www.facebook.com/terms.php>.
- 323 Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e, *et seq.*
- 324 See, e.g., Cal. Lab. Code § 96k; see also N.Y. Labor Code § 201-d.
- 325 See *Sigler v. Kobinsky*, 762 N.W.2d 706 (Wis. Appt. Ct. 2008); *Maypark v. Securitas Security Services USA, Inc.*, 2009 WL 2750994 (Wis. Appt. Ct. 2009).
- 326 *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).
- 327 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.
- 328 la Cour de Cassation
- 329 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.
- 330 TGI Caen, (Nov. 5, 2009)
- 331 The authors wish to acknowledge the contributions of Areta L. Kupchik and Colleen T. Davies to the content of this chapter.
- 332 Pricewaterhouse Coopers LLP, "Social media likes healthcare: From marketing to social business," available at <http://www.pwc.com/us/en/health-industries/publications/health-care-social-media.jhtml>.
- 333 See, e.g., 21 C.F.R. § 202.1.
- 334 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 Website Operators—Part of International Internet Week of Action*, at <http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm191330.htm>.
- 335 See FDA, *Promotion of FDA-Regulated Medical Products on the Internet, Notice of Public Meeting*, 61 Fed. Reg. 48,707 (Sept. 16, 1996).
- 336 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/lsld003.htm>.
- 337 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.fdasdm.com/docs/FINAL%20DDMAC%20Responses%20to%20FDASM\\_Questions.pdf](http://www.fdasdm.com/docs/FINAL%20DDMAC%20Responses%20to%20FDASM_Questions.pdf).
- 338 <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM381352.pdf>.
- 339 See, e.g., <http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/UCM055773#>
- 340 See, e.g., <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/UCM388800.pdf>.
- 341 See <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2011/ucm256922.htm>.
- 342 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.
- 343 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.
- 344 <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM285145.pdf>.
- 345 21 C.F.R. § 314.81 (b)(3)(i).
- 346 See <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM381352.pdf>.

- 347 FDA has issued guidance regarding responding to unsolicited requests for information.
- 348 The Pharmalot blog is now a twitter feed available at <https://twitter.com/pharmalot>.
- 349 Published by Pharmalot, available at <http://www.pharmalot.com/fdas-abrams-long-awaited-social-media-guidance-coming>.
- 350 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.
- 351 See e.g., #TrendingTopic: Privacy Best Practices for #SocialMedia, July 24, 2013, available at <https://cio.gov/trendingtopic-privacy-best-practices-for-socialmedia/>.
- 352 *Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions*, Dec. 23, 2008, available at [http://www.howto.gov/sites/default/files/documents/SocialMediaFed%20Govt\\_BarriersPotentialSolutions.pdf](http://www.howto.gov/sites/default/files/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf).
- 353 *Privacy and Government Contracts with Social Media Companies*, available at <http://epic.org/privacy/socialnet/gsa/>.
- 354 See 18 U.S.C. § 2701 et seq. (1986).
- 355 See, e.g., *United States v. Anderson*, 664 F.3d 758, 762 (8th Cir. 2012) (noting hundreds of Facebook private chats obtained through a search warrant); *United States v. Kearney*, 672 F.3d 81, 84 (1st Cir. 2012) (noting that law enforcement used account and IP address information obtained from MySpace via an administrative subpoena to subpoena defendant's Internet provider for his name and address); *In re Grand Jury Subpoena No. 11116275*, 846 F. Supp. 2d 1, 2 (D.D.C. 2012) (denying anonymous intervenor's motion to quash a subpoena issued to Twitter by a federal grand jury for records pertaining to the intervenor's identity); *United States v. Sayer*, Criminal No. 2:11 cr 113 DBH, 2012 WL 2180577, at \*3 (D. Me. June 13, 2012) (using subpoenas to obtain evidence from Facebook and MySpace); *United States v. Meregildo*, No. 11 Cr. 576(WHP), 2012 WL 3264501, at \*2 (S.D.N.Y. Aug. 10, 2012) (obtaining evidence through warrant issued to Facebook).
- 356 The particularized showing required under the SCA only applies to certain substantive data including (1) contents of wire or electronic communications in electronic storage; (2) contents of wire or electronic communications in a remote computing service; (3) subscriber records concerning electronic communication service or remote computing service; and (4) basic subscriber information. See 18 U.S.C. § 2703(d); see also *In re United States for an Order Pursuant to 18 U.S.C. 2703(d)*, 36 F. Supp. 2d 430 (D. Mass. 1999).
- 357 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.
- 358 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.
- 359 See J. Andrew Moss, *Enhancing the Brave New World of Cyberliabilities and Insurance Coverage*, THE BRIEF, Spring 2013.
- 360 The authors wish to acknowledge the contributions of Maureen C. Cain, Bonnie M. Mangold and Maria Dogaru to the content of this chapter.
- 361 See Chris Wheelock, *A Growing Trend: Social Media As Legal Evidence*, West Michigan Business (July 29, 2009, 12:30 p.m.), [http://www.mlive.com/business/west-michigan/index.ssf/2009/07/a\\_growing\\_trend\\_social\\_media\\_a.html](http://www.mlive.com/business/west-michigan/index.ssf/2009/07/a_growing_trend_social_media_a.html).
- 362 *In re K.W.*, 666 S.E.2d 490, 494 (N.C. Ct. App. 2008); see Sandra Hornberger, *Social Networking Websites: Impact on Litigation and the Legal Profession in Ethics, Discovery, and Evidence*, 27 Touro L. Rev. 279, 302 (2011).
- 363 *People v. Liceaga*, No. 280726, 2009 WL 186229, at \*3-4 (Mich. App. Jan. 27, 2009).
- 364 *Mai-Trang Thi Nguyen v. Starbucks Coffee Corp.*, Nos. CV 08-3354 CRB, CV 09-0047, 2009 WL 4730899, at \*2, 5 (N.D. Cal. Dec. 7, 2009).
- 365 *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 654 (Sup. Ct. 2010).
- 366 *EEOC v. Simply Storage Mgmt. LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010); see Emma W. Sholl, *Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence*, 16 Tul. J. Tech. & Intell. Prop. 207, 225 (2013).
- 367 *R v. Grewal*, [2010] EWCA Crim 2448
- 368 *Locke v Stuart* [2011] EWHC 399 (QB)
- 369 *Nield v. Loveday* [2011] EWHC 2324 (Admin)
- 370 *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at \*9 (Pa. D. & C. 2010); see Lisa McManus, *Waiver of Attorney-Client Privilege or Work Product Doctrine through Social Media*, LexisNexis® Legal Newsroom (Feb. 18, 2011, 9:52 a.m.), <http://www.lexisnexis.com/legalnewsroom/technology/b/legal-technology-blog/archive/2011/02/18/waiver-of-attorney-client-privilege-or-work-product-doctrine-through-social-media.aspx>.
- 371 *Lenz v. Universal Music Corp.*, No. C 07-03783 JF (PVT) 2010 U.S. Dist. LEXIS 119271, at \*7-13 (N.D. Cal. Oct. 22, 2010); see Lisa McManus, *Waiver of Attorney-Client Privilege or Work Product Doctrine through Social Media*, LexisNexis® Legal Newsroom (Feb. 18, 2011, 9:52 a.m.), <http://www.lexisnexis.com/legalnewsroom/technology/b/legal-technology-blog/archive/2011/02/18/waiver-of-attorney-client-privilege-or-work-product-doctrine-through-social-media.aspx>.
- 372 *Juror Declares Defendant "GUILTY" on Facebook*, CBSNEWS (Sept. 2, 2010, 10:49 a.m.), <http://www.cbsnews.com/news/juror-declares-defendant-guilty-on-facebook/>.

- 373 *Dimas-Martinez v. State*, No. CR 11-5, 385 S.W.3d 238, 246, 249 (Ark. Dec. 8, 2011); Suzi Parker, *Arkansas Death Row Inmate Gets New Trial Because of Tweets*, Reuters (Dec. 8, 2011, 3:36 p.m.), <http://www.reuters.com/article/2011/12/08/us-crime-twitter-arkansas-idUSTRE7B72C220111208>.
- 374 Ben Zimmer, *Juror Could Face Jail Time for 'Friending' Defendant*, USA Today (Feb. 7, 2012, 2:34 p.m.), <http://usatoday30.usatoday.com/news/nation/story/2012-02-07/juror-facebook-friend-defendant/53000186/1>.
- 375 Larry Welborn, *Facebooking Juror Kicked Off Murder Trial*, OC Register (Aug. 21, 2013, 1:17 p.m.), <http://www.ocregister.com/news/juror-329708-trial-judge.html>.
- 376 Matt Reynolds, *Blogging Juror Requires Retrial, Burglar Says*, Courthouse News Service (Oct. 10, 2013, 12:47 p.m.), <http://www.courthousenews.com/2013/10/10/61919.htm>.
- 377 *HM Attorney General v. Fraill and Stewart* [2011] EWHC 1629 (Admin)
- 378 *HM Attorney General v. Beard* [2013] EWHC 2317 (Admin)
- 379 *HM Attorney General v. Davey* [2013] EWHC 2317 (Admin)
- 380 *Blaney v. Persons Unknown* (2009)
- 381 *Order of Mr Justice Teare in the High Court of Justice, February 2012*
- 382 The authors wish to acknowledge the contributions of Jesse J. Ash and Paul Llewellyn to the content of this chapter.
- 383 See, e.g., *Fulfilling Regulatory Requirements for Postmarketing Submissions of Interactive Promotional Media for Prescription Human and Animal Drugs and Biologics*, Guidance for Industry, Center for Drug Evaluation and Research, Food & Drug Administration, January 2014, at 2 (hereinafter "FDA Guidance") ("a firm may promote its products through product websites, discussion boards, chat rooms, or other public electronic forums that it maintains and over which it has full control")
- 384 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>
- 385 FDA Guidance at 3.
- 386 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](http://www.boston.com/news/health/blog/2009/09/the_new_england.html)
- 387 The authors wish to acknowledge the contributions of William M. Krogh to the content of this chapter.
- 388 2013 Fortune 500 Are Bullish on Social Media: Big Companies Get Excited About Google+, Instagram, Foursquare and Pinterest, By: Nora Ganim Barnes, Ph.D., Ava M. Lescault, MBA and Stephanie Wright, Charlton College of Business Center for Marketing Research, University of Massachusetts Dartmouth available at <http://www.umassd.edu/cmcr/socialmedia/2013fortune500/>
- 389 *Anthony Fields*, Securities Act Release No. 9291 (2012).
- 390 *Michael Migliozi II*, Securities Act Release No. 9216 (2011).
- 391 See Disciplinary and Other FINRA Actions Reported November 2013 (Charles Michael Matisi (CRD #2650170, Registered Representative, Hauppage, New York)) available at <http://www.finra.org/web/groups/industry/@jp/@enf/@da/documents/disciplinaryactions/p385575.pdf>
- 392 See Financial Industry Regulatory Authority, Misrepresentative and Unbalanced "Tweets" and Other Misconduct, Quarterly Disciplinary Review, July 2011.
- 393 No. 14-cv-1409 (C.D. Cal. Feb. 25, 2014).
- 394 See *SEC v. Christopher A. Black*, Case No. 09-CV-0128 (S.D. Ind., Sept. 24, 2009).
- 395 *SEC v. Presstek, Inc. and Edward J. Marino*, 1:10-CV-10406 (D. Mass. March 9, 2010).
- 396 *SEC v. Berliner*, No. 08-CV-3859 (JES) (S.D.N.Y. April 24, 2008).
- 397 *SEC v. Sarah B. Gangavarapu*, No. CV09-231 (E.D. Tenn. Aug. 31, 2009).
- 398 The authors wish to acknowledge the contributions of Sachin Premnath to the content of this chapter.
- 399 <http://crunchbase.com/company/twitter>
- 400 *Oneok, Inc. v. Twitter, Inc.*, Case Number 4:09-cv-00597 (N.D. Okl. Sept. 15, 2009).
- 401 Stewart, Daxton. *Social Media and the Law*, 2013 Taylor & Francis.
- 402 Id.
- 403 Sam Jones, *HMV workers take over official Twitter feed to vent fury over sacking*, 31 January 2013, available at <http://www.theguardian.com/business/2013/jan/31/hmv-workers-twitter-feed-sacking>
- 404 <http://www.telegraph.co.uk/technology/internet-security/10568019/Syrian-Electronic-Army-hacks-Microsoft-Twitter-accounts.html>
- 405 See generally: <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/18367-trademark-policy#>
- 406 <http://crunchbase.com/company/facebook>
- 407 <http://www.ebizmba.com/articles/social-networking-websites>
- 408 <http://www.facebook.com/terms.php?ref=pf>
- 409 <https://www.facebook.com/help/www/223752991080711>
- 410 See Ryan Davis, *Twitter Helps Usher in New Set of Trademark Perils*, available at <http://www.law360.com/articles/165012/twitter-helps-usher-in-new-set-of-trademark-perils>
- 411 Id.
- 412 <https://www.facebook.com/help/329992603752372>
- 413 <https://www.facebook.com/help/208017472571983>
- 414 Bundesgerichtshof [German Federal Court of Justice], NJW 2002, p. 2031 – shell.de; Hamm Court of Appeals, NJW-RR 1998, 909 – krupp.de.
- 415 <http://instagram.com/about/legal/terms/#>
- 416 See more at: <http://davisudoka.com/blog/view/can-i-trademark-my-awesome-hashtag#sthash.GeE6Ujf5.dpuf>
- 417 *Pinterest Spurs Online Sales – and Trademark Risks*, available at [www.law360.com/articles/402364/print?section=hospitality](http://www.law360.com/articles/402364/print?section=hospitality)
- 418 Id.

- 419 *Id.*
- 420 <http://about.pinterest.com/trademark/>
- 421 <http://www.dailydot.com/business/pinterest-trademark-microsoft/>
- 422 <http://www.dailydot.com/business/pinterest-trademark-microsoft/>
- 423 <http://www.pinterest.com/search/people/?q=Mitt%20Romney>
- 424 15 U.S.C. §1114(1)(a).
- 425 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.”
- 426 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.”
- 427 Stan Hammer, WDVA Court Denies Motion to Dismiss Trademark Infringement Claim Based on Alleged Fictitious LinkedIn Profile, available at <http://virginiaiplaw.com/2013/11/wdva-court-denies-motion-to-dismiss-trademark-infringement-claim-based-on-alleged-fictitious-linkedin-profile/>
- 428 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.
- 429 s10, Trade Mark Act 1994
- 430 Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trademark.
- 431 *Céline Sarl v. Céline SA* (Case C-17/06)
- 432 <https://support.twitter.com/articles/18367-trademark-policy#>
- 433 *1-800 Flowers Inc. v. Phonenames Ltd* [2000] FSR 697
- 434 *Bundesgerichtshof* [German Federal Court of Justice], NJW 2005, p. 1435 – Hotel Maritime.
- 435 *Irvine v. Talksport* [2003] EWCA Civ 423
- 436 Sec. 4 no. 9 German Act Against Unfair Competition.
- 437 Cologne Civil Court, decision of September 16, 2009, file no. 33 O 374/08.
- 438 <http://support.twitter.com/articles/18366-impersonation-policy#>
- 439 <https://support.twitter.com/articles/18366>
- 440 <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/106373-parody-commentary-and-fan-account-policy>
- 441 Jung, Andrew M. (2011) “Twittering Away the Right of Publicity: Personality Rights and Celebrity Impersonation on Social Networking Websites,” *Chicago-Kent Law Review*: Vol. 86: Iss. 1, Article 16. Available at: <http://scholarship.kentlaw.iit.edu/cklawreview/vol86/iss1/16>
- 442 *Anthony La Russa v. Twitter, Inc.*, Case Number CGC-09-488101 (Cal. Super. Ct., San Fran. Co., May 6, 2009).
- 443 <https://support.twitter.com/articles/119135-faqs-about-verified-accounts#>
- 444 Eli Langer, *Respect me—I’m verified on Twitter* (18 November 2013), available at <http://www.cnn.com/id/101200388>
- 445 <https://support.twitter.com/articles/119135-faqs-about-verified-accounts#>
- 446 *Taser International Inc. v. Linden Research Inc.*, 2:09-cv-00811 (U.S.D.C., D. Ariz., April 17, 2009).
- 447 <http://www.techdirt.com/articles/20090421/1310304599.shtml>
- 448 <http://www.bloomberg.com/apps/news?pid=20601103&sid=aR6xHcnBMn9M>
- 449 Richard Acello, *Virtual Worlds, Real Battles: Trademark Holders Take on Use in Games* (1 January 2011), available at [http://www.abajournal.com/magazine/article/virtual\\_worlds\\_real\\_battles/](http://www.abajournal.com/magazine/article/virtual_worlds_real_battles/)
- 450 *Adam Opel AG v. Autec AG* (Case C-48/05).
- 451 *Bundesgerichtshof* [German Federal Court of Justice], decision of January 14, 2010, file no. I ZR 88/08 (not yet published).
- 452 Nir Kossovsky, MISSION INTANGIBLE, Blog of the Intangible Asset Finance Society, September 21, 2009 (quoting Darren Cohen).
- 453 *Eros LLC v. Leatherwood*, No. 8:2007cv01158 (M.D. Fla. 2007).
- 454 *Eros LLC v. Simon*, Case No. 1:2007cv04447 (E.D.N.Y. 2007).
- 455 Registration No. 3,483,253 covering “providing temporary use of non-downloadable software for animating three-dimensional virtual characters.”
- 456 Registration No. 3,222,158 covering “computer graphics services; graphic art design; graphic design services, graphic illustration serves for others.”
- 457 Registration No. 3,531,683.
- 458 Helen Lewis, *Digital money talks, even when it trades in hats and hamburgers* (14 April 2013), available at <http://www.theguardian.com/commentisfree/2013/apr/14/virtual-economies-digital-money-talks>
- 459 <http://lindenlab.com/tos>
- 460 *Id.*
- 461 *Id.*
- 462 *Kierin Kirby v. Sega of America, Inc.*, 144 Cal App. 4th 47 (2006).
- 463 *Marvel v. NCSoft*, No. CV 04-9253 (C.D. Cal. Mar. 9, 2005).
- 464 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.
- 465 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. Further, the “Innovation Act” which passed in the House of Representatives in December of 2013 increases the burden on patent asserters in several aspects. The Innovation Act is not yet law and the Senate has taken up a corresponding bill.