

Global Media and Communications Quarterly

Business, legal and regulatory
trends on four continents

Social media

Contents

Editors' note	2	French Supreme Court invalidates "take down and stay down" rule	26
Corporate social media: a high-level risk assessment	3	Global: Satellites, security and the social graph	30
USA: Tweeting corporate communications	10	USA: <i>Aereo v Aereo</i>	34
Hong Kong: Social media and securities law	13	USA: A hitchhiker's guide to technology, media and cultural innovation in the new frontier states of the American west	37
UK: Beware of advertorials	16	Hogan Lovells Berlinale event focuses on Spanish film production	41
USA: FTC mobile payments report will impact social media-based offerings	18		
Global: Defamation and social media	20		

SPRING
2013

Editors' note

The world increasingly is connected through social media. Social media are interconnected through the Internet. The Internet (and connections to it) consists of a global infrastructure of satellites, fiber-optic and wireless technologies that at its best allow for seamless, real-time, instantaneous communications across the globe. Even for those who consider themselves among the hip, the initiated or the cognoscenti (which reminds us that you will find an excellent discussion of Italian defamation law at page 11), you will learn new terms and concepts in the pages that follow.

For example, while certainly not in earlier editions of Black's Law Dictionary, the word "twibel," is not a typo and is not a phonetic rendering of the word "tribal" as pronounced by Warner Bros' very own Elmer Fudd. So, what exactly is "twibel"? Read on.

In addition to expanding your vocabulary by at least one word, in these pages you will learn about how and why Courtney Love was sued by the estate of her late husband Kurt Cobain, about the cyber-attack vulnerability of global communications satellite networks, about the interplay between public corporations' use of social media platforms and United States and Hong Kong securities regulation – and also about the recent decision of the French Supreme Court invalidating that country's "Take Down and Stay Down" rule applied to websites and hosting services for posting infringing content. You will also find a terrific discussion of recent developments at the intersection of social media and consumer protection law in the United States.

But if subjects like the gravity of cyber threats to our increasingly vulnerable information-based economy, or the prospect that your Facebook page or Twitter feed could become the target of an SEC or other government investigation become too much, consider pure escapism and taking a tour of the "New Frontier States" of the American West, to learn how culture, innovation – and deals – are driving the content sectors of our technology and media worlds.

But for now, let the proceedings begin with Corporate Social Media 101: The Do's and Don'ts of Social Media. We hope you enjoy reading this as much as we all have enjoyed putting it together for you.

Sincerely,

Winston, Dave and Penny



Winston Maxwell

Partner, Paris

T +33 1 5367 4847

winston.maxwell@hoganlovells.com



Penny Thornton

Senior Associate, London

T +44 20 7296 5665

penelope.thornton@hoganlovells.com



Dave Thomas

Partner, Washington D.C.

T +1 202 637 5675

dave.thomas@hoganlovells.com

Corporate social media: a high-level risk assessment

Companies in all industries increasingly are using social media to communicate and connect with consumers, employees, recruits, business partners, investors and other constituents. A recent study by McKinsey & Co. found that 39% of the companies surveyed use social media as their primary digital tool to reach consumers, and that number is expected to increase to 47% within the next four years. The Center for Marketing Research at the University of Massachusetts reported that in 2012, 73% of the Fortune 500 companies used Twitter (up from 62% in 2011), 66% had a corporate Facebook page (up from 58%), and 28% had a public-facing blog (up from 23%). If corporate entities' use of social media for marketing and other purposes is not already ubiquitous, it will certainly become so in the coming years.

Despite the number of legal and other issues implicated by corporate and employee use of social media, businesses are exploring the potential of social media for a number of reasons:



Morgan Stanley plans to allow financial advisers to use Twitter and LinkedIn



- It can be a powerful new marketing, recruiting, and information-gathering tool.
- It can increase customer loyalty, provide access to key demographics, and create “brand ambassadors.”
- It can expand internal knowledge-sharing and serve to flatten an organization, helping to increase employee engagement and buy-in to strategy and policy.
- Ignoring social media can put an enterprise at risk of being surprised or depositioned by injurious behaviors or information.
- They do not wish to allow competitors to pull ahead in productive use of social media. The following are just a few examples of how businesses are effectively implementing social media in their day-to-day operations.

- **Morgan Stanley** recently announced plans to allow its 17,000-plus financial advisors to use Twitter and LinkedIn to communicate with clients and prospects, and has developed “turnkey,” or preapproved, social media content for this initiative.
- **Coca Cola**, one of the sponsors of the London summer Olympics, provided consumers with free tools to create customized music videos that could be shared through social media. More than three million such videos were posted as part of Coca Cola’s “Move to the Beat” Olympic marketing campaign, and the company has reported a surge in the numbers of its Facebook fans and Twitter followers.
- **Nordstrom** maintains one of the most popular corporate pages on Pinterest, a digital pinboarding site that allows users to “pin” any image they find online, where it posts pictures from its catalogs and fashion events. The retailer uses the page to drive traffic to its e-commerce site and to learn which trends and styles its online fans are most interested in.
- Since 2005, **IBM** has used social computing and business conduct guidelines to encourage its workforce to use social media appropriately to collaborate internally and to engage with clients, business partners and other external parties.

While corporate social media activities can create value, the casual culture associated with social media use, as well as the speed with which such capabilities can be used to publish information to a global audience, can substantially increase a business’ legal and related risks, even for those organizations that choose not to actively engage with social media.

Regardless of industry, therefore, companies are well advised first to assess, and then work to mitigate, such risks. Drawing on our work with a variety of clients operating primarily in the United States and Europe, we offer the following inventory of key legal issues and practical tips to help guide businesses and their in-house counsel as they plan their social media strategies.¹

¹ This is a general guide to the social media-related legal issues likely to be encountered by businesses operating in the United States and should not be relied upon as the exclusive source of advice for specific situations. This area of the law and practice is dynamic; for an updated such inventory, contact the authors or the Hogan Lovells attorney with whom you regularly work.

Paying bloggers to create buzz²

In the United States, Section 5 of the Federal Trade Commission (FTC) Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”

Like other forms of advertising, businesses must ensure that promotional messages issued through social media are not false or misleading, even when those communications are not made as part of a formal marketing campaign or crafted by advertising professionals.

In 2009, the FTC updated its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* for the first time in 29 years, requiring bloggers who receive compensation or products in exchange for reviews to disclose that fact. The FTC also clarified that the obligation to disclose a connection between a business and an endorser of its products or services extends to endorsements disseminated through social media sites. The Guides also provide that businesses have a responsibility to monitor the bloggers they sponsor to ensure sure that information included in the blogs is accurate – suggesting that businesses could face liability for deceptive online statements made by third parties over whom they have limited control.

Do spam rules apply?

Social media marketing campaigns may also implicate the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or “CAN-SPAM Act,” which regulates the transmission of commercial email messages. Among other requirements, the Act prohibits deceptive subject lines and requires the inclusion of a clear and conspicuous explanation of how the consumer can opt out of receiving future messages. Although it is primarily directed at email communications, courts have held that the CAN-SPAM Act applies to commercial electronic messages delivered through social media. Accordingly, businesses must be mindful of CAN-SPAM requirements when sending commercial messages to their social media “followers” or “friends.”

Similar rules exist in Europe under the E-Commerce Directive and the ePrivacy Directive

Companies also are increasingly making use of social media “listening” or monitoring services, which allow them to track the online discussion of their brands or products. Some of these tools also enable companies

to integrate social media into their CRM systems and to respond directly to the individuals who are posting about their products or services. Companies that take advantage of such services should consider whether they are using them in a manner that is consistent with consumers’ expectations and respectful of their privacy interests; and if such activities involve consumers located in Europe, companies should review their obligations under European data protection laws.

Tweeting can violate securities regulations³

Under the U.S. Securities and Exchange Commission’s fair disclosure regulation, or “Reg. FD,” public companies cannot selectively disclose material non-public information to market professionals and stockholders. To satisfy Reg. FD requirements, companies typically disclose such information in a broadly disseminated press release or Form 8-K, or a publicized call or webcast that is accessible to the public. Although the SEC has issued guidance indicating that a company may use its website or blog as an FD compliance disclosure tool, disclosures made through a tweet or social media posting have not yet been deemed as sufficiently broad-based to meet Reg. FD requirements, and companies should therefore take steps to limit potential disclosures that may inadvertently violate Reg. FD.



Companies should review their obligations under European data protection laws



The Private Securities Litigation Reform Act of 1995 provides a “safe harbor” for forward-looking statements, as long as those statements are identified as forward-looking and are accompanied by cautionary statements identifying important factors that could cause actual results to differ materially from those discussed in the forward-looking statements. When companies issue forward-looking information via social media – such as through tweets – the safe harbor rules require that the company’s customary cautionary statement be included in the tweet, which can present unique challenges given Twitter’s 140 character limit.

² See “UK: Beware of advertorials”, page 16, *infra*

³ See “USA: Tweeting corporate communications”, page 10, *infra* and “Hong Kong: Social media and securities law” page 13, *infra*.

That picture is copyrighted!

Blogs and social media sites can infringe the intellectual property of others by the unauthorized use of copyrighted pictures, videos, or text in materials posted to the Internet (or even to intranets). If a company permits customers and other third parties to post comments or pictures on its website, blog, or social media page, it can be liable for infringement unless the company qualifies for safe harbor under the Digital Millennium Copyright Act (DMCA) by, among other obligations, removing such content upon notice from a copyright holder that the material is infringing.

Additionally, although the posting of another company's trademark often constitutes fair use, if confusion is likely, such use can result in potential exposure for trademark violations under the federal Lanham Act. In addition, trademark rights can extend in some cases to domain names or website meta tags that might be confusingly similar to the trademarks of other companies. Unauthorized references to or pictures of

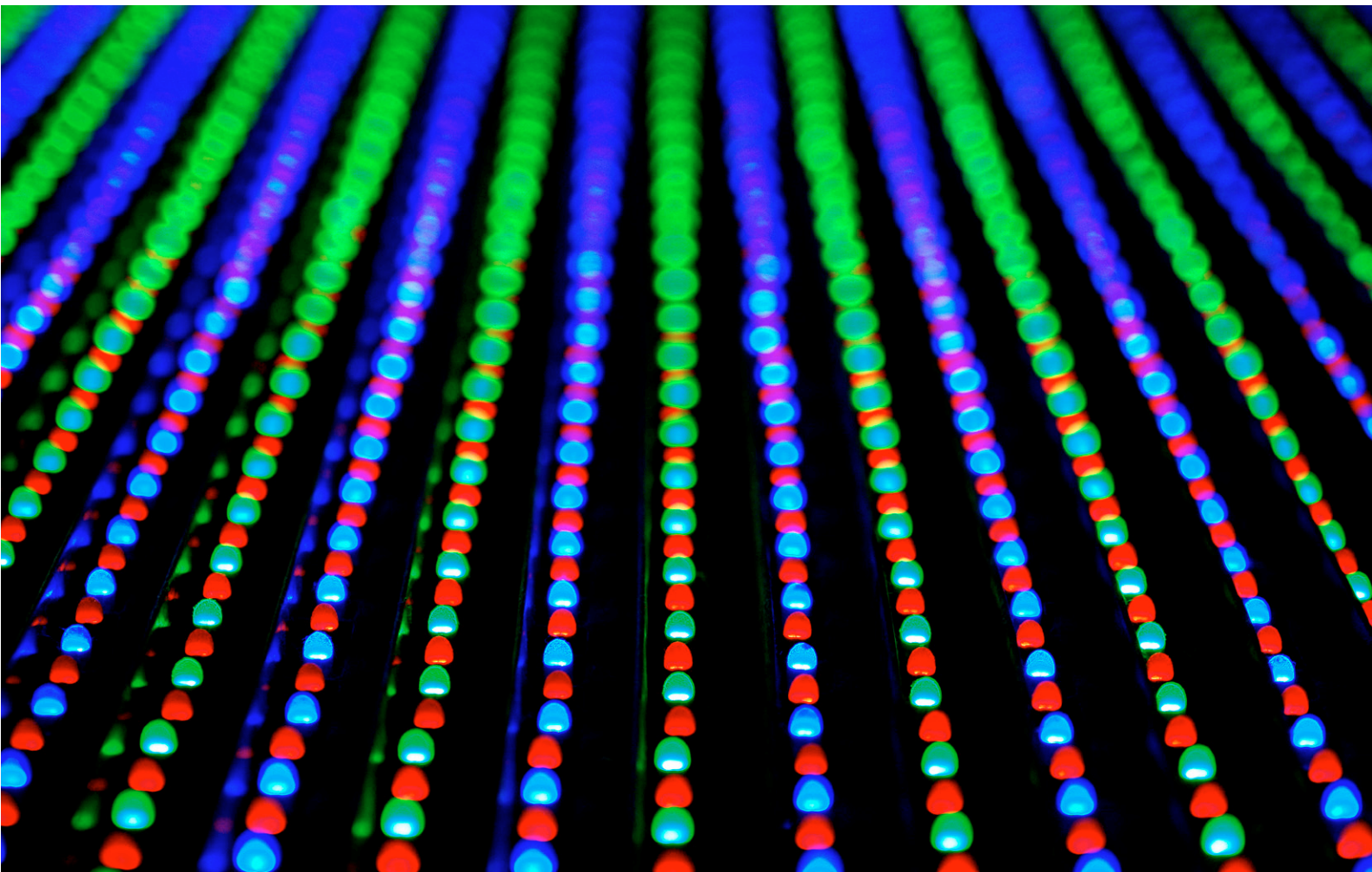
celebrities also can constitute a trademark and/or right of publicity violation.

With respect to protecting its own intellectual property, a company can lose legal protection for trade secrets or other confidential business information that is discussed offhand by employees on social networking sites or message boards available to the public.

Financial and health regulations

By increasing the outlets for communication generally, and for the collection and dissemination of individuals' personal information, the use of social media can expose companies to liability for violations of the privacy rights of employees and customers under a number of theories.

Companies in the financial and medical sectors are subject to privacy and data security requirements under the federal Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA), respectively, which restrict the collection and disclosure of consumers' health and financial



information. GLBA and HIPAA also impose data breach notification requirements on the entities to which they apply. Businesses in these sectors must be especially mindful to ensure that their use of social media does not result in the disclosure of sensitive customer information in violation of their privacy obligations. Additionally, companies in the financial sector should review the proposed social media compliance guidance recently issued by the federal banking agencies.

There are also state laws that apply specifically to social media activities. Prohibitions now enacted into law in Maryland, Illinois, Michigan, and California, and introduced in a number of other states and at the federal level, make it illegal for employers to require access to the personal social media accounts of employees or job applicants. However, employers have the responsibility to balance employee privacy expectations with their own responsibility to manage appropriately their organization, for example by investigating potential wrong-doing by their workforce. Furthermore, regulators in certain industries – including the securities field – have issued rules requiring firms to monitor and archive their employees’ use of social media for business purposes, including when the business-related activities are conducted through personal accounts.



Regulators in certain industries require firms to monitor and archive their employees’ use of social media



Social media postings may also implicate the common law privacy protections recognized by most states, such as prohibitions on the publication of embarrassing private facts about another. Additionally, where companies have made representations – including through privacy policies, consumer terms of use, or commercial agreements with third party entities – regarding the privacy and security of the information they maintain, employees’ use of social media, particularly if not subject to appropriate oversight, may increase the risk that a company will violate its confidentiality obligations.

Employment Lawsuits

Employees claiming unlawful discrimination or harassment can subpoena and point to statements made by other employees through social media to prove their case. Unlike in a traditional discrimination or harassment case, where the allegations as to the actual content of such statements are often subject to conflicting testimony, a jury is unlikely to doubt the content of a discriminatory or harassing statement made and preserved online. Additionally, employers may have an affirmative duty to respond to harassing statements made on third-party social media sites, like Facebook, of which they become aware. Further, as an extension of existing employment law, if a job requires an employee to interact through social media with individuals outside the company, the company could be responsible for harassment perpetrated by the employee if it does not extend and enforce its anti-harassment policy in the online space.

Can I use social media for background checks?

If an employer monitors a social networking site to conduct background checks on prospective employees, or to check up on current employees, it opens the door to claims by rejected applicants or employees fired or denied a promotion that a prohibited factor – such as race and gender, and sexual orientation in some jurisdictions – was used to take that adverse employment action. Additionally, some jurisdictions prohibit the taking of adverse action against a candidate or employee for certain off-duty activities, including tobacco use, any “lawful use of products,” or, in some cases, any legal off-duty conduct. This can present a challenging situation if an employee posts off-duty material that might be objectionable to supervisors, other employees, or members of the general public. Further, if an employer hires a third party to conduct a background check of candidates or existing employees, including by checking those individuals’ social media pages, the employer and third party must comply with specific procedures outlined under the federal Fair Credit Reporting Act and certain state laws.

Social media and union activities

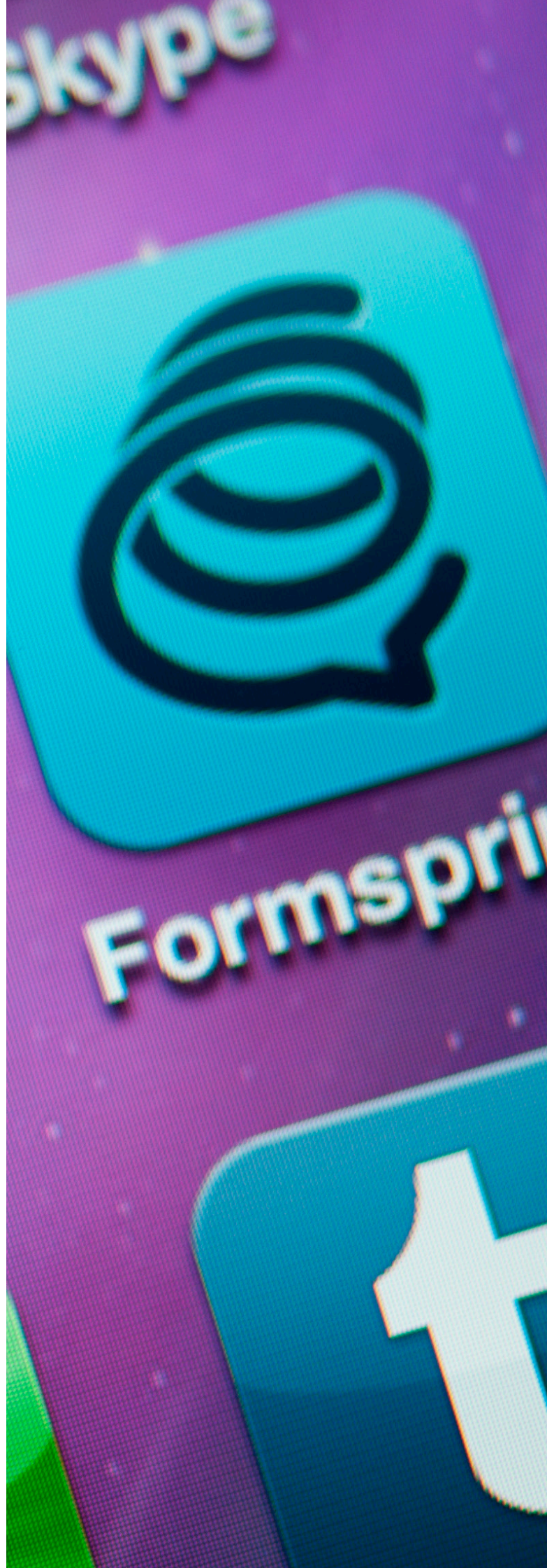
If an employer makes social media use available to its employees, it may not disallow union-related activity – such as discussion of salary, benefits, and other terms of employment – and it could be sanctioned under federal law if it takes any corresponding adverse

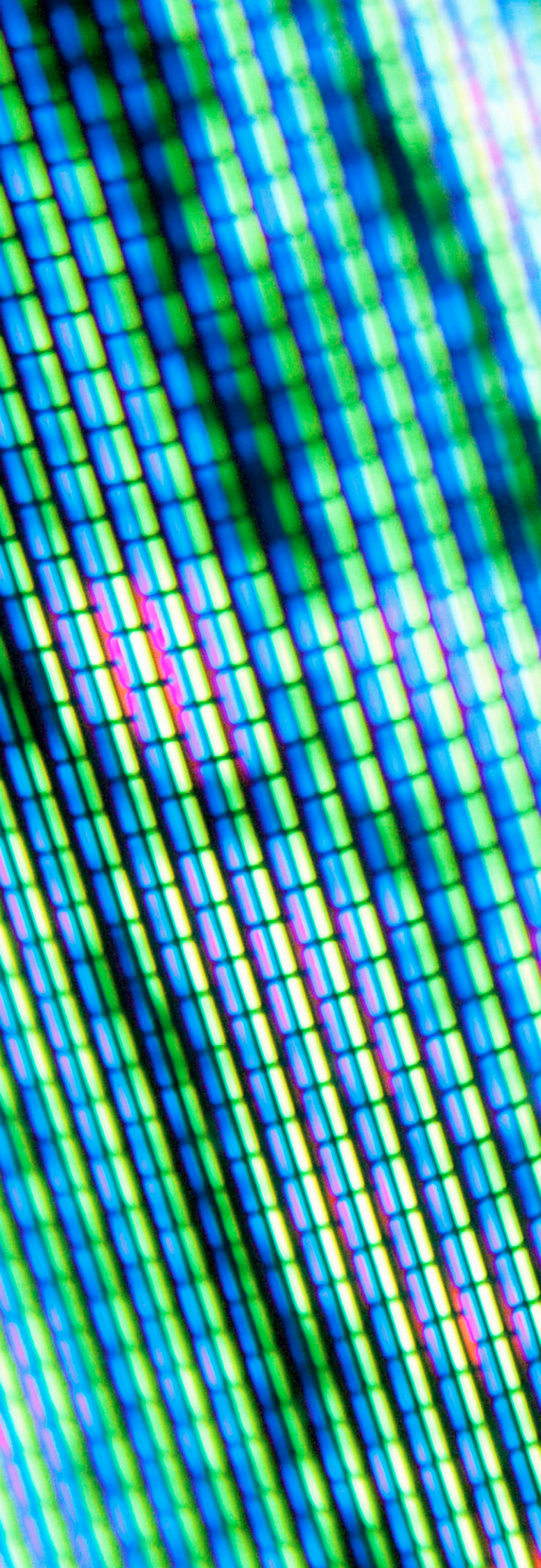
action against employees. The National Labor Relations Board (“NLRB”) has closely scrutinized employer social media policies to see if such policies unlawfully restrict employees’ exercise of rights under Section 7 of the National Labor Relations Act, which protects the right of employees to engage in “concerted activity” concerning issues that affect or relate to their terms and conditions of employment.

“
Companies should implement a scheduled audit or self-assessment process
”

For example, the NLRB found that a policy prohibiting “offensive, demeaning, abusive or inappropriate remarks” – which is not atypical for corporate social media policies – to be overly broad, as it could be interpreted to proscribe protected communications about an employer’s labor policies or treatment of employees. In the recent case of *Hispanics United of Buffalo*, the NLRB concluded that employees’ personal Facebook postings, in which they complained about a co-worker, were protected under the NLRA, and that the termination of the employees on the grounds that the postings constituted harassment and bullying was unlawful. While the validity of the recent NLRB decisions has recently been called into question by the D.C. Circuit Court of Appeals’ finding that President Obama’s recess appointments to the NLRB were unconstitutional, companies would be prudent nonetheless to review their social media policies in light of the NLRB guidance and ensure that they are not overly broad.

In addition, under the common law principle of *respondeat superior*, an employer can be liable for the actions of its employees arising out of their employment. Thus, if an employee posts content to a social media forum that harms a third party, employers can be liable for that harm – in some cases even if the content is not hosted by the employer – so long as this posting arises out of the employment relationship. Further, while employers may only be liable for actions taken by employees in the scope of their employment, the increased interconnectivity of employees through





remote access technologies and mobile devices has drastically changed the concept of what constitutes the “scope of employment” when employees remotely access company materials.

How do I apply a litigation hold?

Rule 34 of the Federal Rule of Civil Procedure governs the discovery of electronically stored information (ESI). In general, social media evidence is considered ESI on par with emails and other electronic files. Like other ESI, businesses must take measures (such as litigation holds) to preserve social media evidence not only at the inception of a lawsuit but whenever litigation is reasonably anticipated. However, the fact that information held on a social media site can be changed or removed at any time – and access to that information may be controlled by a third party – presents particular challenges for discovery involving social media.

Preserving social media evidence may require downloading and retaining it in another format (such as a PDF file). Additionally, in some cases, courts have compelled litigants to produce their social media login credentials when their social media accounts are expected to contain evidence that is relevant to their claims (e.g., photos or status updates that contradict personal injury claims). Other courts, however, have concluded that social media messages and posts are protected by the federal Stored Communications Act and have rejected requests for access to such information in connection with litigation.

International compliance

When utilizing social media internationally, businesses must be sensitive to conflicts of law and design compliance programs tailored to each relevant jurisdiction. For example, the European Union imposes stricter standards than the United States on the level of protection afforded to personal information, and has different standards regarding marketing and defamation claims. The EU also prohibits the transfer of personal information collected from EU individuals to the United States, unless certain protections are applied or the individuals have provided their affirmative consent to the transfer. Other jurisdictions may have similar requirements.

Be mindful of the terms of use

Facebook, Twitter, and other social media sites have their own terms and conditions that apply to users, and which restrict key activities such as advertising on their platforms. These terms typically also regulate promotions (such as contests and sweepstakes) and include restrictions on the use of certain social media platform features, including “liking” a page, as an entry or voting mechanism. A company’s noncompliance with these requirements could result at the least in the suspension or termination of its account, which could have a significant impact on its social media activities and strategy.

Practical Tips

To help mitigate the risks described above, companies, if they have not done so already, should institute a social media policy, making sure the rules are clear and understandable. As with all employment policies, it is advisable to take steps to ensure that all employees have read the policy, for example by having them sign statements acknowledging that they have done so. The policy should establish clear rules to help eliminate misunderstandings and provide a basis for which to discipline employees who contravene the policy. Companies should be careful to avoid policies that are overly broad or that could be deemed to restrict employees’ rights under U.S. labor law to engage in “concerted activity.”

How this policy is deployed outside the US must be determined with the help of local counsel

In addition to establishing a policy, it is important to engage in ongoing oversight of social media activities. Companies should know how their employees are using social media and who is supervising them, and they should take steps to ensure that these individuals are properly trained. Indeed, given the potential for liability, it is imperative that management document and support the implementation of efforts to train the workforce and oversee compliance.

Companies should also implement a complaint process by which both employees and customers have an outlet to report objectionable content. Social media users will often be a “front line of defense” in detecting potentially harmful situations, and it is essential to have an effective complaint and resolution process to diffuse these situations before they escalate.

Finally, companies should implement a scheduled audit or self-assessment process to identify gaps in enforcement of the rules, and in the rules themselves. The organization’s policies should regularly be updated to incorporate lessons learned, to reflect changes in social media platforms, technologies, and strategies, and to narrow existing gaps that could potentially subject the company to additional liability.

With thanks to our colleagues Bret Cohen and Valerie Brennan.



Harriet P. Pearson

Partner, Washington D.C.

T +1 202 637 5477

harriet.pearson@hoganlovells.com



Michael Epshteyn

Associate, Washington D.C.

T +1 202 637 5523

michael.epshteyn@hoganlovells.com

USA: Tweeting corporate communications

During 2012, use of corporate blogging, Facebook and Twitter among Fortune 500 companies increased as companies sought to increase their brand awareness and customer engagement, enhance networking and recruiting, and access key demographics by engaging in social media. According to a study conducted by the University of Massachusetts at Dartmouth, in 2012:

- 73% of all Fortune 500 companies have an official corporate Twitter account with regular tweet activity, which is up from 62% in 2011;
- 66% of all Fortune 500 companies have a corporate Facebook page compared to 58% in 2011; and
- 28% have a corporate blog with regular posts compared to 23% in 2011.¹

While the use of social media has created new opportunities for many companies to reach targeted demographic groups, it also can expose unsuspecting companies and their officers to risks as demonstrated in recently disclosed enforcement action initiated against Netflix and its CEO, Reed Hastings. This article summarizes some of the U.S. securities law considerations and recent guidance that apply to social media use by publicly traded companies.

The SEC alleges that Mr Hastings' Facebook post violates Regulation FD

In December 2012, Netflix and its CEO, Reed Hastings, each received Wells notices from the Enforcement Division of the United States Securities and Exchange Commission (the "SEC") informing them of the intent of the SEC to pursue enforcement action as a result of a July 2012 Facebook post made by Mr. Hastings. The Facebook post congratulated Netflix's content licensing team for exceeding a milestone in monthly viewing hours and contained a positive prediction regarding future monthly viewing hours. Netflix did not file a Current Report on Form 8-K with the SEC, issue a press release or publicly disseminate any other disclosure at the time.

The SEC alleged that Mr. Hastings' Facebook post violated Regulation FD, which prohibits the selective disclosure of material non-public information to market professionals or investors. In a Form 8-K later furnished by Netflix, Mr. Hastings defended his post by claiming both that disclosures made on his Facebook page were "public" given that he has over 200,000 friends who subscribe to his posts, and that the post itself was not "material" information about Netflix.²

The SEC has become more concerned over the use of social media communications

The Netflix action is a reminder that despite the casual and spontaneous nature of communication via social media such as Facebook and Twitter, such communication is still subject to securities laws and regulation such as Regulation FD. To satisfy Regulation FD requirements, companies typically disclose material non-public information in a broadly disseminated press release or Form 8-K, or on a publicized call or webcast which is accessible to the public. In 2008, the SEC issued additional Regulation FD guidance (the "2008 Guidance") explaining how companies may use website disclosure as a Regulation FD compliance disclosure tool. In order to qualify, companies must demonstrate, among other things, the following:

- their corporate website is a recognized channel of distribution;
- posting information on the corporate website disseminates the information in a manner that makes it available to the securities marketplace in general; and
- there has been a reasonable period of time for investors and the market to react to the posted information.³

On April 2, 2013, the SEC concluded its investigation of Netflix and Mr. Hastings and determined not to pursue any enforcement action. Instead, the SEC issued a

¹ The Social Media Surge by the 2012 Fortune 500," Center for Marketing Research, University of Massachusetts at Dartmouth, <http://www.umassd.edu/cmr/socialmedia/2012fortune500/> (last accessed on January 25, 2013).

² Ex. 99.1 to Netflix Current Report on Form 8-K, filed December 5, 2012

³ SEC Interpretive Release No. 34-58288 (August 7, 2008).

Report of Investigation (the “Report”) to provide guidance to issuers regarding how Regulation FD and the 2008 Guidance apply to disclosures made through social media.

The Report states that the principles outlined in the 2008 Guidance apply with equal force to corporate disclosures made through social media channels including Twitter and Facebook – reiterating the fundamental importance of alerting investors in advance to the channels of distribution that a company intends to use to disseminate material information. Companies are also encouraged to identify on their corporate websites the specific social media channels that they intend to utilize for the dissemination of material, non-public information and to give investors and the market the opportunity to take steps necessary to subscribe to, join, register for or review that channel⁴. However, the Report cautions that whether or not a particular Twitter feed or Facebook page qualifies as a recognized channel of distribution of information in compliance with the 2008 Guidance remains subject to a “facts and circumstances” analysis. Finally, the Report clarifies that without advance notice to investors, the disclosure of material, non-public information on the personal social media site of an individual corporate officer employed by a public company is unlikely to satisfy the requirements of Regulation FD even if the individual has a large number of subscribers, friends or other social media contacts.⁵

The guidance set forth in the Report appears consistent with the SEC’s response to earlier reviews of the disclosure of information by executives via social media channels.

In December of 2010, a small internet company, WebMedia Brands, and its CEO, Alan Meckler, appeared to successfully defend tweets via a personal Twitter account against allegations that the tweets violated Regulation FD by applying the 2008 Guidance to the Twitter account. In a comment letter issued to the company, the SEC’s Division of Corporation Finance noted that Mr. Meckler regularly used his Twitter account to discuss pending acquisitions and next quarter results prior to the company’s disclosure of this information in SEC filings. For example, in August 2010, the CEO tweeted: “WebMediaBrands posts its 2nd quarter financials a week from today after market. Conference call is on Thursday.

Rev. growth big.” The SEC comment letter questioned whether the use of the tweets was in compliance with Regulation FD and other SEC rules and regulations.⁶ WebMediaBrands’ response claimed first that the tweets did not violate Regulation FD because none of the tweets concerned material non-public information. As an alternative, WebMedia Brands also claimed that even if the tweets were deemed to be material, Mr. Meckler’s Twitter page was a recognized channel of distribution for information about the company and that the postings disseminated the information in manner that made them available to the marketplace in general because Mr. Meckler’s Twitter feed appears on a blog linked to WebMediaBrand’s corporate website.⁷ After the company submitted its response, the SEC issued a letter stating that it had no further comments.



Mr Meckler regularly used his Twitter account to discuss pending acquisitions



Besides compliance with Regulation FD, communications via social media must also comply with other securities laws and regulations. For example, general anti-fraud rules can apply to any company statements whether written or oral, including tweets or posts. Adhering to these rules in the context of communication via social media platforms can be challenging, because tweets and posts may need to be abbreviated due to character limits of the platforms, as well as the customs and practices that have developed around social media communication. However, issuing short declarative statements using social media, unaccompanied by the kind of qualifying verbiage or additional details that are often included in corporate communications issued by public companies through press releases or SEC filings, creates risks that followers could misinterpret a company’s statements. The company, or individual executive, issuing the tweet or post could be exposed to claims by the SEC or plaintiffs’ lawyers that the substance of the company information contained in the message was not adequately

⁴ SEC Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: Netflix, Inc., and Reed Hastings (April 2, 2013).

⁵ Id.

⁶ <http://www.sec.gov/Archives/edgar/data/1083712/000101968711000062/filename1.htm>

⁷ Id.

communicated. In addition, tweets or posts must still include, or be accompanied by, required disclaimers or reconciliations if they include forward-looking information or adjusted or non-GAAP financial information.



Coordinate the release of information over all platforms



While the SEC's recently issued guidance set forth in the Report reflects a recognition by the SEC of the expanding use of social media by publicly traded companies, companies should continue to exercise caution when using social media and consider adhering to the following practices:

- Require all executives and employees who are authorized to use social media on behalf of the company to have Regulation FD training;
- If the company uses social media outlets to communicate information that could be viewed as material to investors, it should do so in conjunction with traditional forms of disclosure (for example, SEC filings and press releases) and coordinate the release of information simultaneously across all platforms;
- If the company uses different avenues for disseminating company information beyond traditional press releases and SEC filings, the company should alert investors in advance and tell them how and where the company will release such information;
- If the company intends to disseminate company information on social media platforms, the company should consider linking blogs, Facebook pages or Twitter accounts that it intends to utilize to the company's website;
- All posts and tweets by the company or any of its executives that comment on or summarize press releases or earnings calls should include links to the full text of the press releases or webcasts; and

- Adopt, and regularly update, policies to address social media communication by the company, its employees and executives.

The state of the law and best practices in the area of corporate communications via social media is evolving rapidly along with expanding use of social media platforms by companies and their executives. The SEC cases and general legal principles discussed above serve to highlight some of the potential pitfalls that exist in this area. Company counsel, corporate executives, corporate communications teams and other company employees should be mindful of both the risks and opportunities presented by the use social media as an outlet for sharing company information.



Stephen H. Kay
Partner, Los Angeles
T +1 310 785 4627
steve.kay@hoganlovells.com



Lillian Tsu
Partner, New York
T +1 212 918 3599
lillian.tsu@hoganlovells.com

Hong Kong – Use of Social Media Networks by Listed Companies or Companies dealing in Securities

The rapid explosion of social networking has changed the way many companies in Hong Kong promote their brands and distribute their products and services. Yet, along with the benefits, social media networks may expose companies to liability under securities laws in Hong Kong. The Securities & Futures Commission (“SFC”) regulates participants in the securities and futures markets, including The Stock Exchange of Hong Kong (“Exchange”), which in turn regulates companies seeking admission on the Exchange and supervises companies once they are listed. Through the administration and enforcement of a number of laws, the SFC can exercise its statutory powers of investigation and enforcement in cases of corporate misconduct, such as the dissemination of false or misleading information. In this article, we focus on the liability incurred due to unintentional marketing and advertising of financial products as well as the inadvertent disclosure of sensitive information of listed companies on social media platforms.

SFC restrictions on advertising and marketing of financial products

The SFC regulates marketing and advertising of financial products under the Securities and Futures Ordinance (“SFO”) and its subsidiary legislation. Although the issues arising from marketing financial products using social media networks are not specifically addressed, the SFC published a Guidance Note on Internet Regulation in 1999 (“Guidance Note 1999”) which regulates advertisements or documents on securities, investment arrangements and advisory services regardless of the mode of communication or delivery, if such materials are aimed at investors in Hong Kong. The SFC has supplemented the Guidance Note 1999 with additional guidance in respect of specific products including Collective Investment Schemes, Structured Products and Mutual Provident Funds. All these guidelines stipulate that marketing and advertising materials:

- require authorization from the SFC if they target Hong Kong investors;
- cannot be false, biased, misleading or deceptive;
- must be current;
- must contain an appropriate explanation of risks and an unbiased view of the product; and

- the information contained in them is displayed in a prominent place, and is legible or if contained in an audio file, it is audible.

Restrictions on advertising codified under s.103 of the SFO contain a general prohibition against the issue of advertisements, invitations or documents relating to investments, subject to a number of exceptions. A person who commits an offence under s.103 is liable on conviction to a fine of up to HKD500,000 (approximately USD64,100) and to imprisonment for a term of up to three years. In a case of a continuing offence, a person is liable to a further daily fine of up to HKD200,000 (approximately USD25,640) during the time the offence continues.

SFC restrictions on disclosure of sensitive information of listed companies

The SFC oversees the Exchange in its regulation of listing-related matters and has a statutory duty to supervise and monitor the Exchange’s performance of its listing-related functions and responsibilities. Moreover, the SFC may exercise statutory investigation and enforcement powers in a number of circumstances including where it has reason to believe that the management of a listed company has committed misconduct against its shareholders or has misled the public.



Employees increasingly blur the lines between their professional and personal lives



Listed companies and their officers may be held to account for improperly disclosing inside information under the current provisions of the SFO. It is a civil wrong and criminal offence under s.277 and s.298 respectively for a person to disclose false or misleading information about the securities and futures of a company that is likely to induce investment decisions or have a material effect on the company’s share price. A person will be liable if he knowingly disseminates, is reckless, or negligent (as in a civil claim), in disseminating information about his company that is false or misleading in a material fact or through an omission of a material fact. These provisions are

very wide and include any form of dissemination of material in any medium or forum.



A seemingly harmless update may trigger a full scale investigation



Those who suffer pecuniary loss under s.277 have a right to bring a civil action and seek damages. The courts may also impose injunctions in addition to or in substitution for damages. If a person is found to contravene s.298, he is liable to a fine of up to HKD10,000,000 (approximately USD1,282,050) and a term of imprisonment of up to 10 years. Moreover, individuals found in contravention of s.298 (such as a director or licensed officer) may be subject to suspension, disqualification and “cold-shoulder” orders from the courts.

In addition, under the current regulatory arrangement in Hong Kong, the Exchange is responsible for setting the Listing Rules, although these rules must be approved by the SFC. Listing Rule 13.09 give rise to a continuing obligation for disclosure of Price Sensitive Information (“PSI”). PSI should be disclosed to shareholders and the public promptly and in a uniform manner. It is the primary responsibility of a listed company’s directors to ensure that the company complies with all relevant requirements. The Listing Rules do not have the force of law, but the Exchange may impose sanctions including cancellation or suspension of the company’s listing, issuing reprimands, public censure and “cold-shoulder” orders to the offending company or officer.

Implications for companies using social media networks

The provisions highlighted above underscore the risks that are faced by companies (whether listed companies or financial institutions) which use social media platforms. As employees increasingly blur the lines between their professional and personal lives in media communications, a seemingly harmless status update on LinkedIn or Facebook about a project at work may inadvertently trigger a full scale SFC investigation. In light of the draconian penalties under the SFO whereby

directors may be personally liable for the actions of their employees, it is imperative that a company should establish a social media policy with clear and specific guidelines about usage of social media platforms at company level as well as at personal level.

To safeguard against violations of s.277 and s.298, a listed company updating its followers on social media networks should also do so in conjunction with the traditional forms of disclosure (e.g. announcements in newspapers) and coordinate the release of such information simultaneously across all platforms. Additionally, posts of a summary nature should be accompanied by a disclaimer, or a link to a disclaimer. If a company comments on or summarizes a press release, a link of the full text of the press release should also be included. In the event of wrongful inadvertent dissemination of information, the company should immediately issue a public corrective announcement and if necessary, request suspension in trading of its securities.

When issuing promotional material through social media outlets, companies must also keep in mind the SFC Guidelines and the SFO requirements as to what and how information should be marketed. In an informal status update or tweet, it can be easy to overlook an innocuous statement that may be construed as an inducement to invest in a company’s financial products. All employees who are authorised to use social media on behalf of the company should have training on disclosure obligations to ensure they understand these legal requirements. In particular, they should be warned not to engage in conversations on social media networks with third party users. Companies should place disclaimers on these social media platforms indicating the company’s right to remove any third party posts or content.

As for an employee’s personal use of their own social media networks, companies may consider including clauses in employment contracts which deal with the private use of social media networks and make references to policies in the employee handbook. The most common sense approach is to ask employees to “pause before posting”, “differentiate public from private” and to avoid making specific comments on financial products on their private pages on social media networks.



Gabriela Kennedy
Partner, Hong Kong
T +852 2840 5084
gabriela.kennedy@hoganlovells.com



Stephanie Tsui
Trainee, Hong Kong
T +852 2840 5071
stephanie.tsui@hoganlovells.com



UK: Beware of advertorials

The growth of the social media industry within the last decade has been unprecedented. With Facebook now having over a billion active users, and Twitter over 200 million, there is no doubting the influence of these networks. As the social media platforms seek to monetarise their business models there are increasing opportunities for companies to market directly to their consumers. However the close and personal interaction afforded by these sites often treads a fine line between consumer protection legislation and the sites' own terms and conditions.

The Consumer Protection from Unfair Trading Regulations 2008 (the "Regulations") establish the principal consumer protection laws in the UK. The Regulations use the concept of an average consumer, of a particular group, as a benchmark from which to assess whether marketing messages are unfair or misleading. This is particularly relevant for social media as clearly one of its great advantages is the ability to target particular demographic groups precisely. Companies should therefore be aware that when targeting groups that may be considered vulnerable, such as children or the elderly, the content and sensitivity of their communications must be adapted accordingly.

As many social media platforms restrict the length of messages, such as Twitter's 140 character limit, it is likely a message will need to omit information that would be considered material from a consumer protection perspective. The Regulations provide for this by allowing the provisions to be assessed in the factual context of the medium used and any measures taken by the marketer to make the information otherwise available. For this reason companies are advised to include a condensed URL with such messages which gives access to a website containing any further information considered material to that communication.

The Regulations also contain prohibitions against some of the more prevalent online marketing misdemeanours. For example, it is illegal if a marketer uses content in the media to promote a product where it is not clear that the promotion has been paid for, a concept known as an advertorial. Marketers are also prohibited from falsely representing themselves as consumers to create the impression of popular support.

An example of this behaviour would be a hotel owner submitting reviews on Tripadvisor purporting to be a genuine guest of that hotel.

The Advertising Standards Authority ("ASA") is the established means of enforcing consumer protection principles in the context of advertising. It applies the self-regulatory CAP Code (the "Code"), which sets out the rules covering non-broadcast marketing communications in the UK. The basic rule in relation to marketing communications is that they should be obviously identifiable, and should not falsely imply that the marketer is acting as a consumer. Due to an extension of its remit in March 2011, the Code now applies to marketing communications on marketers' own websites, social media sites and even any "user generated content" which has been incorporated into a marketing communication.



Marketing communications should not falsely imply that the marketer is acting as a consumer



Final adjudications are published on the ASA's website, with an upheld complaint often attracting adverse publicity. Marketers who choose to pay for editorial content in social media to promote their brands need to ensure that the author/publisher of that content discloses that payment has been made within the body of the post. The ASA has applied a flexible approach to this requirement, for example by allowing the use of the #ad or #spon on Twitter as an acceptable way for Twitter users to disclose that content has been paid for.

As well as complying with legislative requirements, companies also need to observe the terms and conditions of the social media platforms themselves. These terms can be spread across multiple documents and are often not obvious to locate on the sites. Companies must also be aware that the terms are frequently updated and so continued monitoring is necessary to ensure compliance. In the event these terms are breached sanctions can include the removal of a particular message, suspension of an account

or even account termination. Any such sanctions are likely to have cost implications and be damaging for the brand involved.

“

Sanctions can include suspension of an account

”

The terms imposed by the social media platforms can be highly prescriptive and are not always intuitive. Examples of Facebook’s terms, in relation to promotions, include requirements that promotions must be run through separate applications and that Facebook functions cannot be used to automatically enter competition participants.

Companies opting to use third party social media platforms for marketing and brand development purposes can benefit from vast networks and highly targeted and sophisticated communication tools. However, they must also comply with extensive legislative requirements (including data protection rules) as well as the potentially limiting and frequently changing terms of the sites themselves. This can be a fine line to tread and companies should be alert to the potential pitfalls. However, if managed successfully, the use of social media for marketing can continue to be an extremely valuable tool.

This article was written with the collaboration of Helen McGowan.



Richard Welfare
Partner, London
T +44 20 7296 5398
richard.welfare@hoganlovells.com



USA: FTC mobile payments report will impact social media-based offerings

There has been an explosion in the number and variety of mobile payments services available to consumers in the last couple of years, including several social media-centric payments innovations. New payments products, including peer-to-peer services, mobile coupons, contactless options, and mobile wallets offer consumers and businesses significant flexibility and many new benefits. But regulators are concerned about the prospect of increased risks to consumers. The release of the Federal Trade Commission's (FTC) March 8, 2013 staff report, "Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments," indicates the potential for new and greater regulatory scrutiny of this growing sector. The report discusses the key issues facing businesses and consumers in emerging mobile payments services and highlights the diverse mix of companies comprising the mobile payments ecosystem, including mobile carriers, payment card networks, financial institutions, merchants, and others. It describes three primary evolving concerns, all of

which are relevant to social media-based offerings: data security; privacy; and dispute resolution.

The report – which follows up on a 2012 FTC workshop on the same topic – is a reminder to businesses developing or deploying mobile payments services – and the third parties with whom they share consumer data – that the FTC is continuing to monitor the industry and stands ready to enforce the law against deceptive or unfair practices. The FTC stakes out a claim for broad authority over mobile payments, asserting that it has jurisdiction over mobile phone carriers for non-common carrier activities (e.g., mobile carrier billing) and every other type of company involved in mobile payments except for depository institutions. Therefore, businesses in the mobile payments ecosystem – including social media platform providers, app developers, and advertising networks – should assess their existing data privacy and security practices and other terms and conditions of service to ensure that they are consistent with evolving practices.



Benefits of Mobile Payments/Cost of Regulation

The report notes that mobile payments offer the possibility of significant benefits to businesses and consumers. Merchants stand to benefit from increased competition among payment methods and potentially lower transaction costs. In the social media context, they could also benefit from additional branding and advertising opportunities and the ability to leverage a user's stated interests. For consumers, as the FTC observes, "mobile payments can be an easy and convenient way to pay for goods and services, get discounts through mobile coupons, and earn or use loyalty points." They can also connect users to products more directly via social networking platforms. Additionally, mobile payments may offer "underbanked" persons greater access to financial products. While the FTC emphasizes a need for consumers to have consistent protections (noting discrepancies in statutory protections and business practices based on the product and funding source), it acknowledges that additional regulations may impose costs on businesses, which in turn may negatively impact consumers.

Data Security

The Report indicates that a potential impediment to more widespread adoption of mobile payments services is the perceived lack of security. The technology exists, however, to make mobile payments more secure than traditional payments, and the FTC encourages mobile payments providers to ensure that sensitive financial information is secure as it moves through the payment channel, including through enhanced authentication, end-to-end encryption, and secure storage of the information on mobile devices. The Report also notes that a mix of state and federal laws already impose data security requirements on companies that collect and use financial information. Consumers can also take steps to protect their own data, such as setting passwords to protect sensitive information on their mobile devices.

Privacy

The FTC states that mobile payments services may create significant privacy concerns for consumers. There are many companies involved in the mobile payments ecosystem, and they may be sharing a significant amount of consumer data – particularly in comparison to traditional in-store payments using a

credit or debit card. In the social networking context, highly personalized user profiles pose additional privacy risks when integrated with financial transactions. To address emerging privacy concerns in mobile payments services, the FTC recommends that companies receiving consumers' personal information incorporate privacy protections in each stage of their product development, give consumers choices about data collection, and provide greater transparency about their data collection practices. These steps, along with the FTC's suggestions on data security and dispute resolution (discussed below), will facilitate protection of consumer data and greater trust in the services offered by companies in the mobile payments ecosystem.

Dispute Resolution

Finally, the FTC explains that one of the most significant concerns for consumers using mobile payments services is how to resolve disputes when there are fraudulent or unauthorized charges. Although credit and debit cards have statutory protections that limit consumer liability in the case of unauthorized charges, some mobile payments services may not have such protections. The FTC urges consumers to understand their rights and protections when choosing a mobile payment provider, and for businesses to develop clear dispute resolution policies.

With thanks to our colleague Phillip Berenbroick.



Timothy Tobin

Partner, Washington, D.C.

T +1 202 637 6833

timothy.tobin@hoganlovells.com



Mark Brennan

Associate, Washington, D.C.

T +1 202 637 6409

mark.brennan@hoganlovells.com

Global: Defamation and social media

Across the globe, social networking via the internet is on the rise. In 2012, on average, there were 850 million active users of Facebook each month and 175 million tweets each day. Consequently people's statements, opinions and remarks have the capacity to disseminate more widely, quickly and uncontrollably than ever before. This raises a number of difficult questions in the area of defamation where, up to recently, the law has developed on the basis of more traditional means of communication.

This article looks at how the existing laws of different jurisdictions, the UK, the USA and Italy, treat defamation claims relating to social media, and how policy makers are reacting to ensure that those laws work effectively.

The UK

In the UK, the issue of defamation has recently caught the headlines in two high profile cases. In early 2012, the High Court in *Cairns v Modi* [2012] EWCA Civ 1382 held that a New Zealand cricketer was defamed by the Chairman of the Indian Premier League in a tweet implicating him in match-fixing. More recently, it was reported that Lord McAlpine, the Conservative peer, was pursuing at least 10,000 Twitter users who had re-tweeted false accusations connecting him with the Saville child-abuse scandal.

A New Zealand cricketer was defamed by the Chairman of the Indian Premier League

A critical factor in establishing liability for defamation under UK law is determining who is a "publisher." In UK law, "publisher" is defined very widely, and includes not only those who exercise direct editorial control over published statements ("Primary Publishers"), but also anyone else who makes defamatory comments available to third parties ("Secondary Publishers"). This means that, in the context of social media, there are a number of parties who are potentially liable for the same defamatory statement.

Initial publishers, such as people who send tweets (as in the *Cairns* case) or post messages on blogs or

Facebook pages, will be Primary Publishers liable for defamatory statements they make. A twitterer with few followers, following the logic of *Dow Jones v Jameel* [2005] EWCA Civ 75, might be able to argue that a defamation claim is an abuse of process on the basis that publication was so limited that no real and substantial tort has been committed. But, a quite opposite effect can also occur, given the propensity of defamatory statements to percolate or "go viral" via the internet. In *Cairns*, it was determined by the Court of Appeal that this "percolation phenomenon" is a legitimate factor that can be taken into account by the Courts in assessing damages. This means that a tweet that has only a limited initial audience (Mr Modi's tweet had only 65 immediate publishees) can still result in significant damages. Cairn's was awarded £90,000 and the Court of Appeal upheld that award.

A tweet that has only a limited initial audience can still result in significant damages

Re-publishers will also be Primary Publishers. Therefore, for example, the unqualified re-tweet of a defamatory statement will also result in liability. It is no defence that a publisher is simply repeating a statement made by someone else. This is analogous to the situation in *Cairns* where Cricinfo, an online magazine, published an article based on Mr Modi's tweet. Cricinfo settled out of Court for £7,000 plus costs. Even attaching links to defamatory statements can be a basis for liability (see, for example, *McGrath v Dawkins* [2012] EWHC B3).

Social media websites, such as Twitter and Facebook, will be Secondary Publishers in relation to messages posted on them by their users. However, there are specific statutory defences that they may be able to rely on under section 1 Defamation Act 1996 and Regulation 19 of the E-Commerce Directive, which broadly remove liability where a Secondary Publisher does not have knowledge of the defamatory statement, or reason to suspect that it exists. However, should the website operator obtain such constructive knowledge

of the defamatory statement, for example where it is informed by a prospective claimant, it may be liable unless it then takes steps to take down the defamatory material.



The Defamation Bill may provide clarity for secondary publishers



Internet Service Providers (ISPs) may also be Secondary Publishers of messages posted on the websites that they host, although they can also rely on section 1 Defamation Act 1996 and the hosting defences under s19 of the E-Commerce Directive. However, the Court of Appeal in *Tamiz v Google Inc* [2013] EWCA Civ. 68 treated Google Inc. as a publisher at common law for the period from which it was notified of defamatory comments until those comments were removed and did not consider that Google would have an unassailable defence under Section 1 of the Defamation Act. Unfortunately, it was not necessary for the Court to consider whether Google would have had a hosting defence under the E-Commerce Directive. The current law is still therefore uncertain on liability for ISPs.

That said, the Defamation Bill, which is currently progressing through the House of Lords, may provide some clarity in this area. The Bill includes new provisions expressly aimed at Secondary Publishers. Most significantly, section 10 of the Bill provides that there will be no action against Secondary Publishers unless it is “*not reasonably practicable*” for the claimant to bring an action against the Primary Publisher responsible. What is meant by “*not reasonably practicable*” is not further defined, either by the Bill or in its explanatory statements. While it seems likely that it will include the situation where the identity of the Primary Publisher is unclear, it is less clear that it will apply, for example, where the Primary Publisher has no financial standing.

In addition, the Bill sets out, at section 5, a new statutory defence whereby website operators, as Secondary Publishers, will not be liable for the defamatory posts of users, unless they are given a

formal notice of complaint by a claimant and they fail to respond to it in accordance with statutory regulations. While the content of these regulations has not yet been produced, they are likely to include provisions requiring website operators to identify or provide contact details of persons who posted defamatory statements, as well as obliging them to take action relating to removal of the statements themselves. This is intended to help reduce cases of cyber-bullying and people anonymously posting defamatory statements online.

The USA

In the United States, an increasing number of defamation actions are being brought as a result of statements made on Twitter, Facebook, blogs, and other social media. Journalists, celebrities, and private individuals have all been the target of such suits. One such action brought by a couple in Texas against anonymous contributors to message-board discussions on the website Topix.com produced a staggering \$13.78 million jury award. (This judgment was later thrown out by the court and costs were awarded to the defendants.) *Leshner v. Doescher*, No. 348-235791-09 (Tex. Dist. Ct. June 8, 2012).

Twibel suits abound in the US

A plaintiff alleging libel on a social network may need to satisfy heightened standards imposed by the U.S. Supreme Court to protect First Amendment interests. As in all defamation actions in the U.S., a public-figure plaintiff must prove that the defendant acted with actual malice – that is, with actual knowledge of the falsity of the statement or reckless disregard for the truth of the statement. The standards for cases with private-figure plaintiffs vary state by state, and some states provide for the presumption of damages, falsity, or even fault, in cases that do not relate to a matter of public concern and involve non-media defendants. However, most states at least require proof of the defendant’s negligence.

In one high-profile example of libel-by-tweet (or “Twibel”), Courtney Love was sued by Dawn Simorangkir, a fashion designer known as the “Boudoir Queen.” Simorangkir claimed that Love defamed her on several internet forums including Twitter, most notably in a series of tweets posted in a Twitter “rant.” *Simorangkir v. Love*, No. BC410593 (Cal. Super. Ct. Mar. 26, 2009). Love brought a motion to strike pursuant to California’s anti-SLAPP statute.



Simorangkir claimed that Love defamed her on Twitter

Courtney Love uses anti-SLAPP law

“SLAPP” (or “Strategic Lawsuit Against Public Participation”) is a term used to refer to a lawsuit brought for the purpose of suppressing speech through legal intimidation. Anti-SLAPP legislation enacted by individual states – such as the California statute that Love invoked – is one means to deflect such claims. Twenty-eight states and the District of Columbia have passed legislation to combat the chilling effect of SLAPP suits on the exercise of First Amendment rights.



States have passed laws to combat the chilling effect of SLAPP suits

In her anti-SLAPP motion, Love argued that when a celebrity is the focus of significant public interest her life is a matter of public concern. Love maintained that she made the statements because of her belief in the rights of consumers to warn other consumers about bad business practices. The judge denied Love’s motion, holding that the statements did not involve matters of public interest and that Simorangkir was not a public figure. Love ultimately paid \$430,000 to settle the case – only to be sued for Twibel again by attorneys representing her in a case involving the estate of Kurt Cobain, Love’s late husband.

In contrast with Love’s failed anti-SLAPP challenge, the well-known gossip blog Gawker successfully invoked the California statute in August 2012. The CEO of a technology start-up company sued Gawker for defamation based on a blog post questioning the validity of the CEO’s claims relating to his success in business and his company’s products. The California Court of Appeal affirmed the trial court’s grant of Gawker’s motion to strike based on the anti-SLAPP statute, concluding that the blog post was

constitutionally protected opinion. *Redmond v. Gawker Media, LLC*, No. A132785, 40 Media L. Rep. 2145 (Cal. Ct. App. Aug. 10, 2012).



Case law suggests that CDA immunity would protect a re-tweeter



In the U.S., Section 230 of the Communications Decency Act (CDA) immunizes Internet Service Providers (ISPs) from defamation claims based on the speech of website-users, provided that the ISPs do not contribute to or encourage the creation of the defamatory content. See, e.g., 47 U.S.C. § 230(c)(1); *Jones v. Dirty World Entertainment Recordings, LLC*, 840 F. Supp. 2d 1008 (E.D. Ky. 2012). Because Section 230 provides that no “user” is to be “treated as the publisher or speaker of any information provided by another information content provider,” CDA immunity may also extend to website users who republish defamatory content via, for example, re-tweets on Twitter or Facebook “likes.” See 47 U.S.C. § 230(c)(1). Although “user” is not defined in the statute, case law suggests that CDA immunity would protect a re-tweeter – assuming the original tweet is not edited or supplemented. In *Shiamili v. Real Estate Group of N.Y., Inc.*, for example, a defendant-website administrator who copied an allegedly defamatory comment and reposted it as an unedited “stand-alone post” was held to be immune under the CDA. 952 N.E.2d 1011 (N.Y. 2011). Other courts have similarly held that content forwarded in an e-mail or copied and pasted into a discussion board constitutes information from another content provider under the CDA, thus immunizing the defendant. See, e.g., *Mitan v. A. Neumann & Associates, LLC*, No. 08-cv-6154, 2010 WL 4782771 (D.N.J. Nov. 17, 2010); *Barrett v. Rosenthal*, 146 P.3d 510 (Cal. 2006).

Relatedly, courts have held that publishing hyperlinks to allegedly defamatory content and inserting Facebook and Twitter “share” buttons does not constitute republication of the underlying content that renews the statute of limitations for libel claims. See, e.g., *In re Philadelphia Newspapers, LLC*, 690 F.3d 161 (3d

Cir. 2012); *Haefner v. N.Y. Media, LLC*, 82 A.D.3d 481 (N.Y. App. Div. 2011); *Martin v. Daily News*, 2012 WL 1313994 (N.Y. Sup. Ct. Feb. 10, 2012).

Finally, under the SPEECH Act, which was signed into law by President Obama in 2010, foreign defamation judgments failing First Amendment scrutiny or failing to comport with due process requirements under the U.S. Constitution are unenforceable in U.S. courts. 28 U.S.C. § 4102. This statute is particularly significant in light of the expansive reach of social media, which has the potential to expose U.S. libel defendants to jurisdiction worldwide.

Italy

In Italy, the issue of defamation through social networks is a “hot” topic and there have been many cases recently regarding defamatory comments posted through Facebook, YouTube, Blogs, Twitter, etc. Such cases have concerned first of all the type of liability of the person posting the comment as well as the potential additional liability of the ISP.

Under Italian Law (Article 595 of the Criminal Code), defamation occurs when someone makes publicly

available statements offending the reputation of a third party, which may be an individual or a legal entity (e.g. a company). The elements of the offence are: (i) the injury to someone’s reputation, (ii) the communication to a plurality of people (two persons is sufficient).

Given the specific nature of the Internet, defamation can occur by email (provided that there is more than one addressee), websites and certainly social networks. The Court of Cassation has clarified (Decision No. 25875 of June 21, 2006) that a defamatory statement posted on a website is potentially made available to anyone who can access the Internet and therefore is subject to defamation regulations.

Furthermore, the Italian Criminal Code provides that the crime of defamation is more serious (and the relevant sanction is higher) in the event it occurs through the “press” or “other means of publicity.”

In this respect, there is very recent case law (Court of Livorno, decision No. 38912 of 2 October 2012), which recognized that posting offensive comments on a Facebook personal profile not only represents a defamatory conduct, but is also aggravated by



the circumstance that it occurred through a mean (i.e. the social network) that allows a broad diffusion of the offence, thus applying to Facebook profiles the “other means of publicity” principle described above.

With regard to the criteria to determine jurisdiction in case of online defamation, the Italian Court of Cassation also clarified that in case of defamation through the Internet, the court of the residence of the damaged party has jurisdiction over the case for civil related cases regarding the reimbursement of damages (see Decision 21661 of 13 October 2009) while the court of the accused party’s place of residence has jurisdiction for criminal related cases (see Decision No. 964 of 2011), irrespective of the place where the servers are located or where the information has been made available for the first time (as such criteria, usually applied on the off-line world, are not relevant for online defamation).

Under Italian law, in case of defamation performed through the press, in addition to the liability of the author of the article, there is an additional liability by the “editor” of the newspaper for lack of supervisory control.

Courts have held blog owners jointly liable

Some scholars and court decisions have applied the same principle to the Internet and held web sites and/or web platforms’ providers/owners liable as “editors” for the defamatory contents published on web sites/platforms they manage/own. In particular, owners of blogs have been considered in some court decisions similar to press editors and as such jointly liable for the defamatory content hosted on the blog (see Court of Aosta, decision of 25 May 2006). This interpretation has been overturned by more recent case law which has clarified that the additional liability of the editor only applies to the press, including online newspapers and magazines (see the decisions of the Court of Cassation, Third Criminal Department, of 10 March 2009 No. 10535/2009 and of the Court of Cassation,

Fifth Criminal Department, of 16 July 2010 No. 1907). Consequently, if the content of a defamatory article is published on an online newspaper the editor of such newspaper (along with the author) shall be liable for defamation “through the press”. In this respect, it should be noted that online newspapers are clearly identified as such as they shall be listed in a special register and clearly state their “nature” of newspapers in the online version.

Social media not an editor

With specific reference to social media, Italian courts have excluded the “editorial liability” of the ISP and in general tend to exclude any form of liability due to the mere presence of defamatory content in application of the exemption of liability provided for by the E-commerce Directive (i.e. Directive 2000/31/EC) and its national implementation (i.e. Legislative Decree No. 70/2003). However, according to some court decisions, ISPs can be held liable for the mere fact that the defamatory content has not been removed upon request of the offended party (see Court of Mantua, decision of 24 November 2009). In this respect, there is no clear interpretation by the Italian courts of the provisions set forth in the law implementing the E-Commerce Directive: indeed, according to a strict interpretation of the law (followed by some courts – see Court of Rieti, decision of 27 July 2011) a previous judicial or administrative order is necessary prior to the removal, as the ISP has no possibility to verify the lawfulness of the content to be removed. Other courts have interpreted more broadly the provision and stated that the mere knowledge of the presence of unlawful content (for instance indicated in a cease and desist or warning letter) is enough to oblige the ISP to remove the material reported (see Court of Milan, decision of 20 January 2011 No. 7680; Court of Milan, decision of 19 May 2011 n. 10893; Court of Rome, decision of 13 September 2011).

Some platforms are not considered passive hosting providers

In addition to the above, some courts have also held that websites and social media do not benefit from the liability exemption of the E-Commerce Directive and

1 In March 2012 the order of seizure of such website has been overturned by the Court of appeal.

thus can be held liable when they do not fall under the definition of “passive hosting providers” but rather play a more active role with regard to the information transmitted (for instance, they index or organize in categories the content or provide additional features such as the “related videos/content” function). This interpretation so far has mainly concerned video sharing portals, including YouTube (see court of Rome, decision of 16 December 2009), while there are no precedents so far regarding Twitter or Facebook.

Criminal seizure used to block access

Finally, a new “trend” in the Italian legal system is the seizure (e.g. shut down) of websites hosting unlawful content. The seizure is enforced with an order (granted by criminal courts) addressed to access providers asking them to prevent all users with an Italian IP address from accessing a certain domain or URL: it is therefore a form of geo-blocking. In some cases, the order has affected the entire website, in other only a specific URL. While there are many precedents regarding seizures for copyright infringement and counterfeit activities (see, for example, Court of Cassation, Third Criminal Department, decision of 23 December 2009 No.1055), there is a recent case regarding defamation in which the Court of Belluno, on 26 February 2012, by declaring the defamatory nature of a couple of posts of a website, ordered to access providers to prevent to Italian users the access to the entire website. Such seizure was broadly criticized, in particular for the disproportion of the measure of shutting down an entire website against the offensive nature of only a few pages of it.¹

“

Access providers are ordered to block access to the entire website

”

Indeed, there is a risk that if other Italian courts follow the same principle applied by the Court of Belluno (i.e. shut down of the entire website due to the presence of single defamatory posts) they might make unavailable if not the entire social media website, at least a Facebook profile or a YouTube channel due to single defamatory comments.



Paul Dacam

Partner, London
T +44 20 7296 2615
paul.dacam@hoganlovells.com



Penny Thornton

Senior Associate, London
T +44 20 7296 5665
penelope.thornton@hoganlovells.com



Dori-Ann Hanswirth

Partner, New York
T +1 212 918 3631
dori.hanswirth@hoganlovells.com



Sarah Schacter

Associate, New York
T +1 212 918 3285
sarah.schacter@hoganlovells.com



Marco Berliri

Partner, Rome
T +39 (06) 675823 29
marco.berliri@hoganlovells.com



Marta Staccioli

Associate, Rome
T +39 (06) 675823 15
marta.staccioli@hoganlovells.com

French Supreme Court invalidates “Take down and stay down” rule

In a significant series of three decisions handed down on 12 July 2012, the French Supreme Court ruled that a hosting platform has no obligation to ensure that hosted content that has been previously notified is not later re-posted online by its users.¹ At first sight, the solution adopted by the French Supreme Court seems straight forward, simply applying Article 6-I of Law no. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (“LCEN”). To rule otherwise would lead to imposing on website operators a general obligation to monitor that is prohibited by the LCEN and by Directive no. 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“e-commerce Directive”) that the LCEN transposed into French law.

Yet, the message of the French Supreme Court becomes all the more relevant and significant when it is placed in context. The re-posting of content that is identical or similar to content having previously been notified and deleted was, indeed, one of the topics giving rise to most of the uncertainties before the decisions of 12 July 2012.

Situation before 12 July 2012

First, one ought to recall that the LCEN did not identically transpose the e-commerce Directive. Pursuant to Article 14 of the Directive, “*the provider, upon obtaining [...] knowledge or awareness [of the illicit content], [must act] expeditiously to remove or to disable access to the information.*” Yet, the e-commerce Directive does not specify how the provider becomes aware of the illicit nature of content.

This gap was filled in by the LCEN which established a presumption according to which the operator is aware of the illicit nature of the content when such content is notified to it. Going even further, Article 6-I 5° of the LCEN has very precisely set the conditions to be met by such a notice. These obligations imposed on rights owners wishing to have videos or images removed from a website counterbalance the obligation imposed on the hosting providers to promptly remove content.

In this respect, it is important to provide hosting providers with the means to meet their obligations to act promptly,² which is sometimes strictly punished when content is removed after more than a few days.³ One of the requirements for a complete notice under Article 6-I 5° of the LCEN relates to the precise

location of the notified content because, without this information, the hosting provider cannot in most cases identify and remove the litigious content.

But what is the exact effect of a notice complying with the legal requirements? Is the obligation to promptly remove content met as soon as the provider removes the notified content or must the provider also ensure that the same content is not later re-posted? On websites hosting videos in particular, some Internet users did not hesitate to re-upload videos deemed to be infringing on the website from which they had just been removed.

Equivocal case law on “take down and stay down” until 12 July 2012

Various decisions held hosting providers liable for letting users re-post online content identical to the content that had previously been notified and that allegedly infringed the same intellectual property rights without requesting a new notice.⁴ Some courts even blamed hosting providers for not having implemented sufficient measures that would have prevented the re-posting of the litigious content on the ground that, without such measures, access to the litigious content was not really blocked.⁵



Courts blamed hosting providers for not preventing re-posting of the litigious content



- 1 French Supreme Court, 1st Civil Chamber, 12 July 2012, no. 11-13.669 (Google Inc. and others v. Bac Films and others), no. 11-13.666 (Google Inc. and others v. Bac Films and others) and no. 11-15.165 and 11-15.188 (consolidated appeals, Google Inc. and Aufeminin.com and others v. André Rau, H & K)
- 2 The French courts frequently recall the importance of this provision and the necessity to include specific indications in the notice; see, in particular, French Supreme Court, 1st Civil Chamber, 17 February 2011, no. 09-67.896, Nord-Ouest Production and others v. Dailymotion
- 3 For a recent example, see Paris Civil Court, 29 May 2012, TF1 and others v. YouTube
- 4 Paris Court of Appeal, 9 April 2010, Google v. Flach Films and others; Paris Court of Appeal, 3 December 2010, Dailymotion v. Zadig Production; Paris Court of Appeal, 14 January 2011, Google Inc. v. Bac Films and others; Paris Civil Court, 11 June 2010, La Chauve Souris and 120 Films v. Dailymotion; Paris Civil Court, 13 January 2011, Calt Production v. Dailymotion; Créteil Civil Court, 14 December 2010, INA v. YouTube
- 5 Paris Court of Appeal, 4 February 2011, Google Inc. and Aufeminin.com and others v. André Rau, H & K

However, this position was discussed on the ground that it conflicted with Article 15 of the e-commerce Directive, which prohibits Member States of the European Union from imposing on hosting providers a general obligation to monitor the content of their website.⁶ Furthermore, these decisions may result in “*disproportionate burdens on intermediaries*”,⁷ which would also be unrealistic in light of the volume of information to be filtered and what is technically feasible.

French case law was, in fact, not unanimous on this point as other courts, observing differences between the re-posted content and the similar content that had initially been notified, refused to hold the hosting provider liable for not having prevented the re-posting.⁸ These were notably cases where the videos were not entirely identical (for instance, complete videos instead of trailers or extracts).

Contribution of the decisions of 12 July 2012

The French Supreme Court quashed the appellate decisions holding technical intermediaries liable for letting notified content be re-posted online. These cases

involved either films that could be viewed or downloaded through links available on the Google Videos service, or reproductions of photographs on the website *aufeminin.com* and used by Google Images, in both cases without the consent of the rights owners concerned.

“

Intermediaries do not have any obligation to actively seek illicit content (even though a lot of them do so anyway)

”

Pursuant to the decisions of 12 July 2012, the obligation imposed on hosting providers to promptly remove or block access to re-posted content can only result from a new notice meeting the requirements of Article 6-I 5° of the LCEN. Indeed, the French Supreme Court recalls that such a notice is required for the hosting provider to have actual knowledge of the illicit nature and location of the content in question, without which no action can effectively be implemented.



Thus, the French courts will now no longer be able to impose on hosting providers obligations meant to prevent the re-posting of allegedly illicit and previously notified content. The Supreme Court confirms that “take down and stay down” injunctions fall under the scope of the prohibition of general obligations to monitor laid down in Article 6-I 7° of the LCEN, which transposed into French law Article 15 of the e-commerce Directive. Even though this is merely a reminder of the law, the French Supreme Court mentions that intermediaries do not have any obligation to actively seek illicit content (even though a lot of them do so anyway).

This being said, there is no doubt that rights owners will continue to request the broadest possible injunctions against website operators by relying on the possibility that the French Supreme Court let the lower courts “order a measure of such a kind as to prevent or end the damage related to the current content of the website in question”. Nevertheless, the decisions of 12 July 2012 should encourage lower courts to limit the scope of the injunctions which they may possibly order. The concept of “current content” that has been introduced has a restrictive purpose and should impede preventive measures that would not only concern the content displayed on the day the injunction is imposed, but also future content.

Courts should order more targeted injunctions

The French Supreme Court seems to seek an acceptable and feasible compromise for both rights owners and website operators, which can only be approved. Thus, the lower courts will have to implement a proportionality criterion when ordering a blocking measure. Such a measure, which will necessarily be temporary, must remain proportionate to its purpose.

The French Supreme Court thus follows the indications of the Court of Justice of the European Union, which refers to Directive no. 2004/48/EC of 29 April 2004

6 Pursuant to Article 15(1) of the e-commerce 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”

7 Report of the European Commission of 21 November 2003 on the application of the e-commerce Directive, COM(2003) 702 final, p. 15

8 See, notably, Paris Commercial Court, 27 April 2009, Davis Film v. Dailymotion; Paris Civil Court, 3 June 2011, SACEM v. Dailymotion; Paris Civil Court, 22 September 2009, ADAMI and others v. YouTube

9 CJEU, 24 November 2011, Scarlet Extended SA v. SABAM, no. C-70/10; CJEU, 26 February 2012, SABAM v. Netlog NV, no. C-360/10

concerning the measures and procedures aiming at ensuring compliance with intellectual property rights, to rule that the injunctions that would aim at preventing infringements of intellectual property rights must be effective, proportionate and dissuasive. The European Court held that the European regulations do not allow national courts to enjoin an Internet access provider or social media platform to implement a preventive filtering system of all the electronic communications passing through its services that would indistinctly apply to all its customers, at its exclusive expenses and without any limitation in time. National authorities are thus prohibited from adopting measures that would force an operator to actively monitor all the data of all its users to prevent any future infringement of intellectual property rights.⁹



The fight against infringements is a never ending process



What's next?

As Margaret Thatcher said, one may have to fight a battle more than once to win it. This seems the case here, whether from the standpoint of the rights owners (who have to send a notice each time content infringing their rights is posted online) or of the website operators (who must remove the content upon obtaining actual knowledge of its existence on the website). In this respect, the fight against infringements of intellectual property rights is a never-ending process as it is very difficult to prevent Internet users from infringing intellectual property rights by re-posting content that was previously removed by operators.

A significant number of hosting providers already implement proactive measures to fight against the illicit activities of the users of their websites. It is generally possible to easily and quickly report online the existence of content that may infringe intellectual property rights and request such content to be removed. The main online video platforms also offer the possibility for rights owners to provide fingerprints of the videos concerned for the operator to attempt to prevent the re-uploading of content it may identify as illicit by comparing it to the print.

The decisions of 12 July 2012 confirm the fact that hosting providers do not have the obligation to implement such measures as it is the rights owners' duty to send the necessary notices. Nevertheless, these measures are welcome when they are technically possible and show the good faith of the operators of websites, which do not seek to benefit from counterfeiting. These decisions should thus not be interpreted as an encouragement towards website operators to stop applying such measures. They are, indeed, frequently mentioned by courts as being positive and lead courts to refuse to order against responsible and diligent operators unnecessary injunctions insofar as such injunctions would be redundant with existing measures, or less efficient.¹⁰

Furthermore, European authorities are seeking to reduce, if not definitively end, the practices of intellectual property rights infringement. The European Commission launched, on 4 June 2012, a public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, the purpose of which was to gather the opinion of the different parties concerned on the best practices in this field.¹¹ The way rights owners should inform hosting providers of illicit content and the reaction that these intermediaries should adopt are part of the addressed issues. This consultation is now closed since 11 September 2012 but its results are not yet known. A legislative development on this point, in particular a revision of the e-commerce Directive, should not be excluded.

**Christine Gateau**

Partner, Paris

T +33 1 5367 1892

christine.gateau@hoganlovells.com

**Christelle Coslin**

Senior Associate, Paris

T +33 1 5367 1824

christelle.coslin@hoganlovells.com

¹⁰ See Paris Civil Court, 13 September 2012, TF1 and others v. Dailymotion, which acknowledges the reliability of the solutions implemented by the website; see also, Paris Civil Court, 29 May 2012, mentioned above

¹¹ See http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_fr.htm and <http://ec.europa.eu/yourvoice/ipm/forms/dispatch>

Global: Satellites, security and the social graph

In our age of telecommunications convergence, and the infusion of social media throughout all communications, it is unremarkable that satellite communications would face the same risks of cyber attack as are facing the telecommunications industry generally. With our increased reliance on space technology, these risks present real issues and vulnerabilities.

The nature of satellite communications, however, presents some significant structural differences and susceptibilities for cyber terrorism, hacking and risk avoidance.

Satellite cyber-attack terminology

“Soft” kills: informational, reversible or temporary disabling without destruction.

“Hard” kills are permanently disabling or destructive. While hard kills can include missile attacks, air raids or sabotage, they also include various directed energy attacks, including microwave, particle beam, electromagnetic pulse weapons and laser weapons, but can also include self-destruction commands or actions intended to cause loss of satellite control.

Jamming includes use of electronic interference or signals that overpower communications channels. Jamming is deliberate interference with satellite signals.

Deception reflects the forgery or interception of transmissions to or from the attacking space system.

Advanced Persistent Threat (APT) is typically used to refer to a cyber threat by a group, including a foreign government, with both the capability and the intent to effectively and persistently target a specific entity for attack.

Some general facts ¹

1. The U.S. Navy faces 110,000 cyber attacks every hour, or more than 30 every second.
2. One-third of attacks globally are said to originate from China.
3. Nearby in Tokyo, in an effort to develop its defenses against cyber attacks, Japan concluded its first government-approved hacking contest in February 2013.

Satellites as a target

There are approximately one thousand military and civilian satellites orbiting earth today, all of which are potential targets for cyber attack. These satellite systems are subject to cyber attack through “soft” kills to the satellite, but can also take the form of “hard” kills to the satellite system. Soft kills seem likely to be the most common approach since they may keep hidden the source of the activity, but they can equally paralyze or destroy a satellite.

Soft kills seem to be the most common approach

Satellite systems are susceptible to cyberattack through both their ground-based and space-based components, through manipulation of their electronic links, in any number of ways and system components:

- Taking control of (or nullifying the ability to control) a satellite
- Deliberately interfering with satellite transmissions, by jamming, denying, degrading, or forging (counterfeiting) signals, either from the ground or from other satellites
- Key targets of communications link attacks are satellite uplink (transmitting information from ground station to satellite) and downlink (transmitting information from satellite to ground systems) facilities
- Accessing (and potentially leaking) satellite-produced or stored information

¹ <http://www.voanews.com/content/japan-first-government-sponsored-hacking-contest/1597014.html>
<http://www.v3.co.uk/v3-uk/news/2238996/akamai-study-finds-a-third-of-all-cyber-attacks-originate-from-china>
<http://thenextweb.com/us/2012/12/05/us-navy-sees-110000-cyber-attacks-every-hour-or-more-than-30-every-single-second/>



- Implanting computer virus and logic bombs into satellite information systems
- Compromised chipsets, ground systems, internet links and other system components or interfaces can be the vehicles for satellite cyberattack
- Compromising other satellite or terrestrial based networks used by the satellite, or with which the satellite can in turn interfere
- Using the above techniques to lay the <http://www.voanews.com/content/japan-first-government-sponsored-hacking-contest/1597014.html>

Military, civilian and commercial satellites serve a broad range of services including voice, data and internet communications, broadcast services, mapping, space exploration, global positioning, meteorology, surveillance, navigation, and emergency services. In some cases, the satellite produced or stored information can be highly sensitive, putting national security at risk.



Taking control of the satellite can disable the nation's security and defense



In the most extreme of cases, taking control of the satellite can disable the nation's security and defense

in the case of attack. In the past, there have been reports of satellite jamming tests and laser blinding of U.S. reconnaissance and French satellites, as well as a variety of other antisatellite capability demonstrations believed to be by the Chinese government.² In January 2012, a virus infecting Japan Aerospace Exploration Agency computers caused information to be sent to the International Space Station.³

In the case of commercial satellites, the cyber-risk can be analogous to taking down a significant part of the telecommunications grid in a terrorist attack, or to political censorship by shutting down social media in-country.⁴ Further, as commercial satellites become more connected with the internet, the cybersecurity risks increase and there is a greater diversity of concerns.

Satellites and the "Mainframe" paradigm. As in the case of terrestrial, computer based cyber attacks, in the original computer network paradigm there was a walled off, limited-access computer mainframe model that provided significant protection against security breach. While some satellites are similar to the mainframe model in various respects, the vulnerability of satellites to attack has increased exponentially as technological interference, control and hacking attacks have also exponentially increased in recent years.

Some interference, as has been seen by global satellite operators and their customers, is a result of targeted governmental political actions to block dissenting

political perspectives. Recent examples of this include Iran's satellite jamming of news broadcasts of the BBC, Voice of America and Radio Free Europe not only into Iran, but also into countries ranging from Morocco to Eastern Europe to Indonesia⁵ as well as incidents originating from Cuba, Libya, Indonesia, Syria, Bahrain, China, Kyrgyzstan and Uzbekistan.

“
Satellite jamming is a growing scourge and a threat to the vital flow of free information

Peter Horrocks, Director BBC Global News

Historically, satellite operators have been reluctant to publicize cases of intentional interference, but the rapid increase in incidents has caused the industry to issue public statements to bring attention to the problem. Satellite fleet owner Eutelsat has reported that jamming incidents doubled between 2010 to 2011, increased again threefold between 2011 and 2012, and reported 340 incidents in the first ten months of 2012.⁶ Middle-east operator Arabsat similarly recorded a three-fold increase in jamming attacks during the 2011 to 2012 period.

Threat to control of satellites. At another level, access to satellite control has been hacked. According to the November 2011 Report to Congress by the US-China Economic and Security Review Commission (November 2011 Report) at least two U.S. government imaging satellites, Terra EOS and Landsat 7 have “each experienced at least two separate instances of interference consistent with cyberactivities against their command and control systems.”⁷ In the case of the Terra

2 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress, First Session, November 2011 (U.S. Government Printing Office, Washington: 2011) (November 2011 Report), pages 213-14, footnotes 306-307.

3 <http://www.space.com/14231-japan-space-agency-computer-virus.html>

4 One recent example is that of India, where more than 250 websites have been blocked, Google and Facebook ordered to pull content, and legal action threatened against Twitter if it did not delete certain accounts. See <http://www.theatlantic.com/international/print/2012/08/when-is-government-web-censorship-justified-an-indian-horror-story/261396/>

5 / Press Release, Eutelsat, dated October 4, 2012. “Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators” <http://www.eutelsat.com/news/compress/en/2012/html/PR%206212%20interference%20iran/PR%206212%20interference%20iran.html>

satellite, the hackers “achieved all steps required” to assume control of the satellite, although actual commands were not issued. The November 2011 Report observed:

If executed successfully, such interference has the potential to pose numerous threats, particularly if achieved against satellites with more sensitive functions. For example, access to a satellite's controls could allow an attacker to damage or destroy the satellite. The attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission. A high level of access could reveal the satellite's capabilities or information, such as imagery, gained through its sensors. Opportunities may also exist to reconnoiter or compromise other terrestrial or space-based networks used by the satellite.⁸

The November 2011 Report found that the techniques deployed in these activities were consistent with authoritative Chinese military writings: “according to *Military Astronautics*, attacks on space systems ‘generate tremors in the structure of space power of the enemy, cause it to suffer from chain effects, and finally lose, or partly lose, its combat effectiveness’” and that “[o]ne tactic is ‘implanting computer virus and logic bombs into the enemy's space information network so as to paralyze the enemy's space information system.’”⁹

In the case where U.S. or other countries' satellites have been accessed, it is unknown whether and what cyber activities are implanted in these satellites as a pre-staging for an Advanced Persistent Threat.

“
State-sponsored hackers are patient and calculating. They have the time, money and resources to burrow in and wait. You may discover one breach only to find that the real damage has been done at a much higher level¹⁰

Robert Mueller, FBI Director

6 <http://www.bbc.co.uk/mediacentre/latestnews/2012/201112wsjammingconferencehtml>

7 November 2011 Report, p. 216.

8 November 2011 Report, p. 216.

9 November 2011 Report p. 217, and footnote 321.

10 CNN Money http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm?iid=EL

Satellites as a Tool of Social Media. Satellites historically were based on non-IP communications technologies, and hence less susceptible to cyber-attack. As satellite missions move toward an end-to-end interoperable IP environment, they become more susceptible to attack at the same time that cyber-sophistication has increased.

As satellite communications mimic terrestrial communications in their function and role, in addition to the “mainframe” risks, satellites and their users face the same, more extensive risks as do terrestrial communications users that do not have the “mainframe” isolation or defenses. Connecting satellites to the internet significantly increases satellites’ and their related ground systems’ vulnerability to (low-cost) cyber-attack. With the increase in satellites’ roles in individual communications and broadcast services, the risks to safeguard of personal data, financial information, and other business data increases.

While satellites are often thought to provide more secure communications than their terrestrial wired and wireless counterparts, as hackers continue to increase their sophistication there is no reason to believe that cybercrimes for satellites will not increase with their terrestrial counterparts.

“

Eutelsat has added an anti-jamming technical solution

”

Preparing to Meet the Threat. “The cybersecurity challenge is complex and dynamic, especially because there is a powerful upside to the continued embrace of digitalization and connectivity.”¹¹ The integration of these susceptibilities into space systems further exacerbates the inherent special cyber sensitivities of satellite systems. Security measures that may have been sufficient in the past will not meet the cyber threats of the future. In the past, for unsophisticated or unintentional sources of interference, increasing the power of the satellite uplink could overwhelm the interference source. But as in the case of the terrestrial world, as cyber technologies increase in sophistication, a more sophisticated tool kit is needed to combat the new cyber risks.

New tools that specifically cater to the satellite industry are being made available to satellite operators. Eutelsat, which has been a vocal opponent of intentional interference, has added an anti-jamming technical solution to one of its scheduled Middle Eastern satellites, where it has met with significant intentional signal interference. This protective technology has previously been cost-prohibitive according to Eutelsat. But a new public-private cooperative initiative, the European Space Agency’s (ESA) Flight Heritage Program, has facilitated the addition of new satellite de-risking technologies to flight hardware. In addition, the ESA program has considered critical satellite needs to avoid impacts to mission-critical components.¹²

While these new developments may help counteract cybersecurity threats for new satellites, owners of existing satellites should develop plans to assess risks and determine if there are cost-effective solutions available. Our firm and other consultants prepare guides to help operators conduct network assessments to determine the level of risk that exists, assess its existing resources, put plans in place to monitor potential cyber attacks and make decisions regarding the cost-effectiveness of available countermeasures. No guarantees exist that a particular operator’s system will not be chosen for a cyber attack. But measures can be taken to reduce the level of risk, and to understand the current situation and provide meaningful analyses to the managers of the company making decisions on where to allocate resources. And it is only a matter of time before customers insist upon defensive programs being in place.



Randy S. Segal
Partner, Northern Virginia
T +1 703 610 6237
randy.segal@hoganlovells.com



Steven M. Kaufman
Partner, Washington
T +1 202 637 5736
steven.kaufman@hoganlovells.com

11 Harriet Pearson, *Cybersecurity: The Corporate Counsel’s Agenda*, BNA Privacy & Security Law Report, 11 PVLR 1792, 12/17/2012.

12 Peter B. de Selding, “Eutelsat to Field Test New Anti-jamming Capability,” January 28, 2013, *SpaceNews* p. 4, Volume 24, Issue 4.

*Aereo v. Aereo*killer: New York and California District Courts Disagree on What Constitutes a Public Performance Under the Copyright Act

Technology continues to evolve at an ever increasing pace, often leaving in its wake lawsuits that require the application of laws enacted before the technological advancements occurred. Perhaps it is not too surprising, then, that in struggling to apply “old laws” to “new technologies,” courts sometimes reach contrary conclusions.

A recent example of this phenomenon involves two companies that provided their subscribers with access to copyrighted content over the Internet using virtually identical technologies. Although neither service was licensed by the copyright owners, one service was preliminarily enjoined, but the other was not as the courts grappled with the issue of what constitutes a public performance under the Copyright Act.

In *American Broadcasting Companies, Inc. v. Aereo, Inc.*, 874 F.Supp.2d 373 (S.D.N.Y. 2012)¹, copyright owners of broadcast television programming sought to preliminarily enjoin a service that allowed defendant Aereo’s subscribers to contemporaneously view those same programs over the Internet. One of the liability theories asserted by the plaintiffs was that Aereo’s retransmissions of the broadcasts constituted “public performances” of the plaintiffs’ copyrighted programs. The District Court for the Southern District of New York denied the motion, however, finding that the

plaintiffs had not demonstrated a likelihood of success on the merits based on the Second Circuit’s prior construction of the Copyright Act’s “transmit clause” in *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) (“*Cablevision*”). [2]

“

The cable operator split the programming data into two streams

”

The *Cablevision* case involved a cable operator’s “RS-DVR” system that allowed subscribers to record cable programming on central hard drives housed and maintained by the cable operator at a remote location. To provide the service, the cable operator split the programming data it received from cable networks into two streams: one of which was routed immediately to its customers (as authorized by the content owners), while the other stream was used to create a unique, unlicensed “playback copy” that was stored on a portion of the hard drive allocated to a particular subscriber following the subscriber’s request that the programming be recorded. This allowed numerous subscribers to



watch the very same programming via the RS-DVR, but through the playback of unique copies of the programming, each of which was accessible only by a particular subscriber.

The district court originally concluded that the RS-DVR playbacks constituted unauthorized public performances because the cable operator was transmitting the same program to members of the public. *Id.* at 135. The Second Circuit, however, determined that “a transmission of a performance is itself a performance,” *id.* at 134, and that the focus of the inquiry, therefore, should be on the potential audience “of a particular transmission,” rather than on the potential audience “of the underlying work (i.e., ‘the program’) whose content is being transmitted.” *Id.* at 135. Thus, because each RS-DVR playback transmission (i.e., “performance”) was “made to a single subscriber using a single unique copy produced by that subscriber,” the court held that the performances were not “to the public.” *Id.* at 139.



Each user is assigned a dime-sized antenna



Aereo’s service achieves a similar result as the *Cablevision* RS-DVR, but through a different technological platform that assigns a single, dime-sized antenna to a particular user at a particular time, such that no two subscribers are assigned the same antenna at the same time. Each antenna separately receives the incoming broadcast signal, which then goes to a unique directory before being sent to the subscriber over the Internet.

The plaintiffs argued that the antennas function collectively, and effectively act like a “community antenna” that simply passes along a broadcast signal to the public. *Aereo*, 874 F.Supp. at 385. The court, however, found that the antennas function independently of one another, *id.* at 381, and that “the copies Aereo’s system creates are not materially distinguishable from those in *Cablevision*...” *Id.* at 385. Accordingly, it determined that the plaintiffs were unlikely to succeed on the merits in light of the *Cablevision* decision.

The Aereokiller Case

A few months later, and 3000 miles to the west, many of the same plaintiffs sought to preliminarily enjoin Aerokiller, another entity that captured and retransmitted broadcast programming using individual mini-digital antennas. *Fox Television Stations, Inc. v. BarryDriller Content Systems, Plc*, 2012 WL 6784498 (C.D. Cal Dec. 27, 2012). Aereokiller opposed the plaintiffs’ preliminary injunction motion, arguing that its service was technologically analogous to the service found to be non-infringing in *Aereo*. *Id.* at *1. The District Court for the Central District of California, however, refused to apply Second Circuit law and issued a preliminary injunction, holding that Aereokiller’s retransmissions were public performances that infringed the plaintiffs’ copyrights. *Id.* at *2. [3]

Based on prior Ninth Circuit law, and the language and legislative history of the “transmit clause,” the district court rejected *Cablevision*’s focus on the “transmission of a performance.” *Id.* at *3-4. Instead, the court reasoned that the focus should be on “the performance of the copyrighted work, irrespective of which copy of the work the transmission is made from.” *Id.* at *4 (emphasis in original). As the court practically observed:

“Very few people gather around their oscilloscopes to admire the sinusoidal waves of a television broadcast transmission. People are interested in watching the performance of the work. And it is the public performance of the copyrighted work with which the Copyright Act, by its express language, is concerned. Thus, *Cablevision*’s focus on the uniqueness of the individual copy from which a transmission is made is not commanded by the statute.” *Id.* (emphasis in original).

1 This case was previously discussed in the GMC Watch by Dan Brenner and Steve Kay.

2 The “transmit clause” provides, in relevant part, that “[t]o perform or display a work ‘publicly’ means... to transmit or otherwise communicate a performance or display of the work... to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.” 17 U.S.C. § 101.

3 Recognizing its disagreement with Second Circuit law, and refusing to assume that other circuits would cleave to its analysis, the Aereokiller court limited the geographic scope of the injunction to the Ninth Circuit. *Id.* at *7.



Appeals may bring clarity

Both cases are now on appeal, and oral argument already has been heard by a Second Circuit panel whose questions during the oral argument indicated it was troubled by the outcome in *Aereo*. Whether that will ultimately lead the court to revisit the *Cablevision* decision or to seek some basis for distinguishing *Aereo* from *Cablevision* – such as the fact that the *Cablevision* retransmission service (as opposed to the RS-DVR service) was licensed by the plaintiffs, even though that license does not appear to have been material to the decision – remains to be seen.

As this edition of the GMCQ was about to be published, the Second Circuit, in a 2-1 ruling that will be the subject of an upcoming article, affirmed the district court's denial of a preliminary injunction over a strong and lengthy dissent by Judge Chin, who also authored the district court opinion that was subsequently reversed by the *Cablevision* court. This could lead to a split between the circuits (if the Ninth Circuit affirms the contrary *Aereo* ruling) and, ultimately, possible Supreme Court review.



Tony Basich
Partner, Los Angeles
T +1 310 785 4626
anthony.basich@hoganlovells.com

USA: A hitchhiker's guide to technology, media and cultural innovation in the new frontier states of the American West

More than Facebook, Twitter and Instagram, social media as a concept covers applications, techniques and issues as diverse as online gaming, mobility, bandwidth-intensive applications, deep-packet inspection and personally identifiable information. Ultimately "social media" is about redefining the nature of all dimensions of relationships, narrow and broad – sometimes for the better, sometimes not. Here, we take a brief trip across the American West to explore the frontiers of social media and tech innovation.

Our journey starts at the farthest western edge of the continental United States, in California.



California no longer has the lock it once had on innovation



Leaders of the world's tech economy, such as Apple, Google, HP and a stable of tech companies that are not global household-names, were founded in dorm rooms and garages at and around Stanford University. Just a short drive south of San Francisco, and an even shorter drive over the mountains from the Pacific shore, you cannot get much farther west in the lower 48 than Stanford and its greatest progeny, the Silicon Valley.

Hollywood – the film capital of the world – is 350 miles south of Stanford and Palo Alto, and is itself only 12 miles from the Pacific Ocean. (So, to be technical about it, Hollywood actually *is* farther west than Silicon Valley).

But while California contributes to the world more than its share of tech innovation and content, California no longer has the lock it once had on innovation, or on announcing those innovations to the world. Companies generating the news and buzz and innovation that drive investment, policy initiatives, regulatory reactions and legal developments on a global basis increasingly have their coming out parties a bit further East – although not *that* far.

If your business depends on understanding what tomorrow's technology and content drivers will be, remember these four places from the American West: Las Vegas, Nevada; Park City, Utah; Aspen, Colorado; Boulder, Colorado; and Austin, Texas.

These are not just places to gamble and ski or wash down smoked brisket with cold Lone Star beer. These are places where the future is being made. Now.

Nevada

Consumers Electronics Show, Las Vegas, Nevada.

South and east from Palo Alto, and north and east from Hollywood lies our first stop in the big square states: Las Vegas, Nevada.

Las Vegas is home to more than gambling, neon and memories to be taken to the grave. It is also home to the Consumer Electronics Show. Held in early January before full recovery from the indulgences of Christmas and New Year's, CES, as it is known, spills out of almost every patch of convention and floor space along the Strip. This year at CES the world saw self-driving cars; desktop (and larger) 3D printers that allow us to mass produce high-quality machine parts, jewelry, toys and a host of other objects (one 3D printer on display even produced a house) and ultra HD (or 4K) televisions, the next era in picture quality.



This year at CES the world saw self-driving cars



If you are interested in the hottest electronics products and services (aside from Apple), including those that use massive amounts of wireless network capacity, as well as those that strike fear into the hearts of consumer protection and privacy advocates and regulators, then CES should be on your list.

<http://www.cesweb.org/>

Utah

Sundance Film Festival, Park City, Utah

We move next to the north and east of Las Vegas to Park City, Utah (about 100 miles from the spot where in 1869 Leland Stanford presided over the driving of the "golden spike" completing the transcontinental railroad) and the Sundance Film Festival. Founded 35 years ago, and lovingly and meticulously developed by Robert Redford and his dedicated crew at the non-profit Sundance Institute, Sundance has become one of the world's great artistic and cultural events – and not just because it flashes the

greatest concentration of celebrities, wannabes and paparazzi on the planet during the festival's 10-day run.

Sundance has grown from a smallish film show case to a leading global power in international cinema and premium content attracting tens of thousands to Utah's alpine paradise. Though not having an interactive or "social" media focus *per se*, with the introduction of approximately 150 films on screens in Park City and beyond, Sundance films have become staples in the theatrical release, premium video-channel and the video after-markets.

“

Sundance has grown from a smallish film show case to a leading global power

”

Sundance itself has become a major forum for exploring complex and controversial political and cultural issues, such as poverty, racism, the Bosnian war and the US invasion of Iraq. Sundance also is a success story of the public-private partnership model that would not be possible without major support from the state of

Utah and a host of major philanthropic benefactors and corporate sponsors as diverse as video content companies including Time Warner, YouTube and DirecTV, as well as Chase Bank, Southwest Airlines and Acura.

At Sundance, deals get done, films get funded and buzz abounds.

<http://www.sundance.org/>

Colorado

The Technology Policy Institute of the Aspen Institute, Aspen, Colorado

Continuing our trek eastward, the next stop is Aspen Colorado – specifically the Aspen Institute's Technology Policy Institute. One of the great technology think tanks, and set in one of the world's great destinations, the Technology Policy Institute is a source of ideas, research and wisdom on some of the most pressing economic and technology policy questions of the day. Every August, Aspen hosts its Technology Policy Forum, and hosts a handful of other technology events throughout the year. Recent forums have explored the economics of spectrum auctions, the economics of file sharing, online film and music sales and efforts to combat online piracy.

<https://techpolicyinstitute.org>



Silicon Flatirons Center for Law, Technology, and Entrepreneurship, University of Colorado, Boulder, Colorado

For those who can't get to Aspen in August, consider heading a little farther east, to Boulder, Colorado – home of the main campus of the University of Colorado (and *alma* mater of Sundance founder Robert Redford) and the Silicon Flatirons Center for Law, Technology, and Entrepreneurship.

The Center's mission is "to elevate the debate surrounding technology policy issues; support and enable entrepreneurship in the technology community; inspire, prepare, and place students in these important areas [and to serve] as a source for new ideas [regarding technology policy]." Hosting a dozen or more seminars and conferences with thought leaders in media, technology, policy, law and entrepreneurship, the Center grapples with the real problems of translating the promise of technology into reality – and confronts the multifaceted consequences (intended and otherwise) that result once technology is loosed. Topics throughout the year are broad and deep, ranging from start-up financing, monetization of content on the web, challenges in patent law and policy in the software and applications sectors and cybersecurity. Hogan Lovells partners are regularly invited to speak at Silicon Flatiron events.

<http://www.siliconflatirons.com/index.php>

South by Southwest ("SXSW"), Austin, Texas

Farther to the south lies the last leg on our Western state journey, Austin, Texas. Austin is the home of the University of Texas Longhorns, Stevie Ray Vaughan, Dell Computer and the South by Southwest Festival (SXSW).

Texas is large and diverse (and a Texan might note it is bigger – geographically speaking of course – than France). But Austin, the only state capital in today's road trip, is different from the rest of Texas – and SXSW, which started as "just" a music festival, has grown into one of **the** global events in electronic media, making SXSW different too.



SXSW is the edgiest stop on our Western state journey



A cross between a smaller CES and an interactive Sundance (complete with the smell of mesquite smoke and a roots-blues and country-music soundtrack), SXSW is a required stop for those who earn their livings anywhere in the content or interactive media ecosystem. Stretching for 10 days (this year from March 8-17) with different tracks for film, music and interactive media, SXSW, like Sundance and CES, is a place where deals get done and buzz is everywhere. SXSW is the edgiest stop on our Western state journey, but what you see at SXSW today will be downloaded to your tablet or smartphone tomorrow.

<http://sxsw.com/>

Conclusion

Things are happening out West, on the new frontier for social media and high tech innovation. It might be too late *this year* for CES, Sundance, or SXSW, but it is not too early to plan for next year. And it's certainly not too late to get to Silicon Flatirons for one of its high-quality programs.



Ari Fitzgerald

Partner, Washington D.C.
T +1 202 637 5730
ari.fitzgerald@hoganlovells.com



Dave Thomas

Partner, Washington D.C.
T +1 202 637 5675
dave.thomas@hoganlovells.com



Hogan Lovells Berlinale event focuses on Spanish film production

For the tenth straight year, Hogan Lovells hosted its annual Film Panel during the “Berlinale” film festival. This year’s event focused on film financing opportunities in Spain and was hosted in cooperation with the Spanish Embassy in Berlin.

Spain has for a long time been a high-profile location for film productions that have received international awards. For example, during the Berlin International Film Festival 2012, the Spanish co-production, “Les Adieu à la Reine”, was the opening movie. Furthermore, the documentary, “Sons of the Clouds: The Last Colony”, by producer and director Álvaro Longoria was screened during the Berlin International Film Festival 2012, starring Oscar winner Javier Bardem. Or “The Milk of Sorrow” by the Spanish producer José Maria Morales, which was awarded the Golden Bear at the International Film Festival 2009. In light of the foregoing, the Ambassador of Spain, His Excellency Pablo Garcia Berdoy, personally gave a word of welcome to the members of the Panel as well as to all those in attendance. The Ambassador of Great Britain, Simon McDonald, also attended the event.

Christoph Wagner and Christiane Stützle, leading the international film team at Hogan Lovells, were happy to welcome our high-ranking Panel from the Spanish film industry: Susana de la Sierra (General Director, ICAA), Carlos Rosado (President, Spain Film Commission), Álvaro Longoria (producer and director), Pilar Benito (Managing Director, Morena Films), José María Morales (founder and producer, Wanda Films), Emilio Palomar and Rafael Moreno (Bankinter), Christine Rothe (Managing Director, Constantin Film), Alexandra Lebret (Managing Director, European Producers Club) as well as Patricia Sánchez (Hogan Lovells Madrid).

In the context of the panel discussion, presented by Christiane Stützle, it was revealed rather quickly how attractive Spain is for film productions. Susana de la Sierra and Carlos Rosado outlined the variety of locations, the fantastic infrastructure, and the comparatively low costs. Álvaro Longoria and José María Morales, two highly profiled producers from Spain, confirmed that impression and encouraged investors by explaining that for each project, you will find the right partner in Spain. Furthermore, Christine Rothe,



Left to right: Christiane Stützle, H.E. Pablo Garcia-Berdoy (Ambassador of Spain) and Dr. Christoph Wagner

who produced for Constantin Film “The Perfume” in Spain, mentioned the fantastic shooting conditions and the highly professional film teams in Spain, which also leads to a really good benefit-cost ratio.

Spanish tax shelters

Talk of the day was the Spanish tax shelter model, which grants an attractive production incentive of up to 30% on the production budget. The legal framework was presented by Patricia Sánchez, tax lawyer of Hogan Lovells Madrid, together with Emilio Palomar and Rafael Moreno of Bankinter and Pilar Benito from Morena Films, who also explained from her own experience that the tax shelter model works exceedingly well.

After the Panel, some 300 guests from the international film industry enjoyed good networking opportunities and Spanish food and drinks at the reception which followed. The event was accompanied by a live performance of famous Flamenco dancer Ana Maria Amahi.



Christoph Wagner

Partner, Berlin

T +49 30 726 115 211

christoph.wagner@hoganlovells.com



Christiane Stütze

Partner, Berlin

T +49 30 726 115 234

christiane.stütze@hoganlovells.com



Left to right: Susana de la Sierra, Carlos Rosado, Christiane Stütze, Álvaro Longoria, José María Morales and Christine Rothe

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante	Denver	Jakarta*	New York	Silicon Valley
Amsterdam	Dubai	Jeddah*	Northern Virginia	Singapore
Baltimore	Dusseldorf	London	Paris	Tokyo
Beijing	Frankfurt	Los Angeles	Philadelphia	Ulaanbaatar
Berlin	Hamburg	Madrid	Prague	Warsaw
Brussels	Hanoi	Miami	Riyadh*	Washington, DC
Budapest*	Ho Chi Minh City	Milan	Rome	Zagreb*
Caracas	Hong Kong	Moscow	San Francisco	
Colorado Springs	Houston	Munich	Shanghai	

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses. The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising.

© Hogan Lovells 2013. All rights reserved. 8980_EUn_0413

* Associated offices