Social Media:

A Brave New World of Engagement

Exploring the Emerging Risk, Legal and Regulatory Issues in Social Media

David F. Katz, Eliyahu E. Wolfe

The social media revolution has been credited with bringing down dictators, has made billionaires out of twenty-year-old computer programmers, and has commoditized personal information and altered perceptions of privacy on a scale never before seen. This revolutionary and transformative period for communications will necessarily have far-reaching consequences on interactions between organizations and individuals. Businesses are diving into the world of social media to exploit unprecedented opportunities to communicate effectively with targeted audiences; to gain information about customers, employees, and investors; and to obtain customer, client, employee, or investor feedback through new forms of interactive communication. Yet businesses large and small must be prepared to confront a gamut of evolving legal and regulatory issues unique to social media. Traditionally understood risk management techniques must be implemented by businesses seeking to exploit the benefits of social media without falling prey to an ever-changing landscape of legal and regulatory pitfalls.

Transformative Times in Communications

Social media developments are transforming how we communicate on multiple levels. Social media provides tremendous business and political applications through opportunities for digital marketing, brand development, and content diversity. Societally, social media has made it easier for individuals to engage in collective action – for example, the Arab Spring movement that saw the overthrow of governments in 2011 in Libya, Tunisia, and Egypt, and the failed 2009 Green Revolution in Iran– and has led to the rise in citizen journalism, which has, in turn, exponentially increased alternative media outlets and created a true twenty-four hour news cycle.

Perhaps easiest to observe on the personal level, social media provides individuals the capacity for personal digital branding, and provides unprecedented human freedom in communication and knowledge sharing. An ever-growing number of individuals - including students, teachers, employees, executives, retirees, and attorneys – are consuming and contributing to new forms of media on the go. During a typical daily commute, one can readily access, review, and even edit an entry on the online resource Wikipedia (which is increasingly being regarded as a legitimate resource, in comparison, the Encyclopædia Britannica announced in March 2012 that its final printed edition would be the 2010 edition). Networking professionals rely on their LinkedIn accounts both to organize their contacts in a 21st century version of the Rolodex and define their own professional identities to clients, customers, and employers. The 2013 In-House Counsel New Media Engagement Survey, which culled data from 379 in-house attorneys, reveals the pace and extent of this continuing communications revolution. From 2012 to 2013, survey respondents who read general business media on their smartphones

increased from 42 percent to 53 percent; over half the respondents stated that quality of law firm blogs influenced their hiring decisions; and 65 percent of respondents had used Wikipedia to conduct company and industry research. http://insidecounselsurvey.com/2013-infographic/.

The effects of these transformative developments in communication can be either enormously constructive or destructive. A successful viral video campaign can allow an organization to get millions of individuals to watch and re-transmit an advertisement without investing in an expensive advertisement campaign. Yet if not approached properly, this same viral video campaign could put the organization at risk for copyright or trademark infringement, or violation of federal truth-in-advertising laws or FTC disclosure regulations. Likewise, an executive touting her professional accomplishments on LinkedIn may inadvertently blur the line between her company's carefully constructed corporate identities and thereby provide fodder for an opposing party to "pierce the corporate veil" in a lawsuit. The key takeaway from these and numerous other hypothetical and real-world examples of social media use is that whether social media is a boon for business or a pitfall is based on a carefully appreciation for the new medium's inherent risks.

Emerging Legal and Regulatory Issues in Social Media: Illustrations of Risks and Benefits of Social Media from Securities Regulation, Information Security, and Employment Law

Securities Regulation

Since the Great Depression, publicly traded companies have needed to be vigilant about complying with Securities and Exchange Commission regulations. The impact of communications developments and the rise of social media on a company's compliance regime was perfectly illustrated by the fallout from Netflix's Chief Executive Officer Reed Hastings for his July 3, 2012 Facebook post that Netflix had streamed 1 billion hours of content in the month of June 2012. This post prompted a "Wells Notice" and an investigation into whether Mr. Hastings's post violated Regulation FD and Section 13(a) of the Securities Exchange Act of 1934. Ultimately the SEC determined not to pursue an enforcement action, and instead issued Release No. 69279 on April 2, 2013 that lays out certain steps for avoiding the violation of securities regulations while using social media.
http://www.sec.gov/litigation/investreport/34-69279.pdf

The fact that an almost year-long SEC investigation was triggered by a mere posting on Facebook, a website that hundreds of millions of users consider a personal website, should be enough of a wakeup call for all publicly trade companies to re-evaluate their social media policies at regularly scheduled interval to ensure they are updated in how securities regulations are catching up with the rise of social media.

Information Security – Safeguarding Against Hackers and Cyber-Spies

Two April 2013 stories illustrate the importance of enacting comprehensive risk management policies. On April 22, 2013 the Associated Press's Twitter feed was hacked and a fake tweet that the there had been two explosions at the White House and that President Barack Obama had been injured led to the Dow Jones Industrial Average falling more than 150 points in a two-minute span. After the AP denied the story, stocks rebounded. Strengthened security for the news outlet's Twitter feed could be instrumental in preventing future havoc on the financial markets and misinformation campaigns by bad actors. That same month, the Boston Police Department used its Twitter feed to proactively correct misinformation that had spread rapidly in the wake of the drama surrounding the frantic chase and apprehension of the Boston bombing suspects. (For more, see
http://insidecounselsurvey.com/2013/04/23/risk-management-in-social-media/;

http://online.wsj.com/article/SB10001424127887324874204578437360241416842.html?KEYWORDS=Michael+Chertoff).

The Workplace (and Labor Regulations) Now Extends Beyond Mortar and Bricks

Just as new regulations related to the Internet and social media must be followed to comply with the 1934 Securities Exchange Act in the 21st century, compliance with the National Labor Relations Act, first passed in 1935, requires careful vigilance and updating internal policies. For example, Section 7 of the Act provides employees, *inter alia*, the "right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." Employers need to be careful to comply with evolving applications of Industrial Age regulations. The National Labor Relations Board has repeatedly held that electronic limitations on negative commentary violate the Act. *E.g., Dish Network Corporation*, 359 NLRB No. 108, slip op. at 5, (Apr. 30, 2013) (employer's social media policy unlawful, in part, for prohibiting "disparaging or defamatory comments about" employer); *DirectTV U.S. DIrectTV Holdings, LLC, et al.* 359 NLRB No. 54, slip op. at 2, 6 (Jan. 25, 2013); *Costco Wholesale Corp*., 358 NLRB No. 106, slip op. at 2 (2012). In addition, in the last two years twelve states have enacted laws restricting employers from demanding access to potential or current employees' social media; most recently, New Jersey enacted a social media privacy law (A2878). Dozens of other states are considering similar legislation. Illinois' Right to Privacy in the Workplace Act, first passed in 2012 and amended in 2013 to permit employers access to certain information about professional social media accounts, demonstrates how quickly this area of law is evolving.

On the flip-side, employees need to be educated about what *not* to put on the Internet in a way that does not infringe on their freedom of speech and their rights under the National Labor Relations Act. Actions by employees outside the confines of the office could be extremely damaging to the employer. Just some examples include: an employee's LinkedIn or Facebook post to a racist, sexist, or otherwise offensive article can embarrass the employer in the public eye and give rise to a hostile work environment or discrimination claim; a Facebook "friend request" to a co-worker, or from a manager to a subordinate, may likewise be seen as creating a hostile work environment; an employee may disclose confidential business information through a blog post, leading to negative outcomes in subsequent IP litigation. Additional pitfalls may appear based on how employees use employer-supplied technology. For example, an employer needs to understand what reporting requirements are triggered if an employee is using employer-supplied technology to view child pornography.

As the *Dish Network Corporation* and *DirectTV* decisions show, employers walk a tightrope when they attempt to regulate social media but failure to enact a comprehensive risk management policy for social media would be akin to sticking the corporate head in the sand like the proverbial ostrich. Although social media presents complex and evolving issues to employers, failure to enact comprehensive risk management policy for social media could expose the employer to liability, threaten its intellectual property, or lead to public humiliation.

Risk Management for the 21st century.

The common lesson that can be gleaned from the SEC investigation faced by Netflix, the juxtaposition of the AP Twitter feed being hacked with the successful use of social media by the Boston Police Department, and the NLRB rulings in *Dish Network*, *DirectTV*, and *Costco*, is that businesses must create and maintain comprehensive policies to channel the benefits of social media without

increasing their exposure to legal and regulatory risks. By applying risk management principles to social media, businesses can effectively balance the potential costs and benefits of social media and steer clear of avoidable risks.

A first step in any risk management analysis requires the identification of sources of risk and the extent of the risk, which then allows businesses to put in place strategies and procedures to mitigate those risks that cost less than the risk itself.

In ever example cited in this article, the risk posed to the organization came from human actors. Indeed, the most common sources of risk are human. Employees, executives, competitors, and anonymous hackers all present potential threats to businesses; whether through innocent mistakes or intentional sabotage. Businesses must be prepared to confront the wide range of risks posed by different human actors and must ensure the appropriate policies are in place to mitigate specific risks. Whereas employees and executives will likely need to be trained in how social media use can implicate securities regulations and employment law issues such as hostile work environment or discrimination claims, strengthened security measures may need to be created and checked to protect against hackers.

8 Steps to Apply Risk Management to Your Business

The eight steps listed below are a starting point that any organization can use as guideposts to creating a risk management strategy appropriate for the individual risks and opportunities facing a particular organization. Once a risk management strategy is created for an organization, it is essential that the risk management strategy be both utilized and re-evaluated on an ongoing basis.

1. Conduct audit of exposure to risks posed by social media *and* opportunities presented by social media.
2. Adopt clearly defined social media strategy that incorporates risk analysis, crisis management, and good data analytics.
3. Memorialize social media policies through the help of qualified counsel.
4. Train employees on risks posed by social media often.
5. Monitor social media sites and legal developments concerning social media.
6. Create and follow a plan for engaging with various target groups – e.g., customers, clients, or investors.
7. Discipline employees, within the limits of employment law and regulations, who are causing employer reputational harm, threats to intellectual property, or creating uncomfortable work environment.
8. Prepare and plan for litigation and discovery, which now will often involve the equally treacherous world of discovery into electronically-stored information.

David Katz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office where he leads the Privacy and Information Security Practice Group. Elie Wolfe is an associate in Atlanta and a member of the Firm's Litigation Group.