CLM 2017 National Retail, Restaurant & Hospitality Conference
February 22 - 24, 2017
Grapevine, Texas

The Good, The Bad and the Ugly: Strategies for Addressing Social Media Use by Customers, Companies and Employees

I. The Good – Any Press is Good Press- Opportunities and Challenges with Dealing with Social Media Comments

A. Favorable Commentary
   1. Use of comments beyond posted sites- "echo-chambering" the compliment.
   2. Respond/not to respond- does comment warrant a form of response
   3. Relevant examples from various websites- trip advisor, etc.

B. Favorable Announcements
   1. Posting Company Successes
   2. Marketing – Inviting independent, third- party critique- credibility

C. Tricks and Traps for Responding to Negative Social Media Posts
   1. Never Delete, or ignore negative comments
   2. Screenshots to document
   3. Forward to legal for certain type of comments before response

D. Determining How to Respond
   1. If cleared to respond, do so quickly, short, concise, to content of comment only.
   2. Use professional, pleasant tone
   3. Do not engage commenter in "debate"
   4. Remove irrelevant or inappropriate comments (racist; spam)
   5. Block users who abuse the site

E. Determining if Follow Up Should Be Personal
   1. Thank commenter, apologize for negative experience, ask for private exchange.
   2. Ask for and gather more private information via pm, or t/c.
   3. Public Follow up on line, IF issue is resolved

4. Publicize private options for customers to reach company.

II. The Bad- When The Public Reach Costs you- Civil Liability Exposure for Social Media Messaging-

Instant reach to literally millions of consumers. What's not to love? Companies are racing to better engage their customer base through the use of social media. But, unlike in politics, is it really accurate to say that any press is good press? While social media interaction can lead to increased familiarity with your company, and is capable of enhancing a company's brand, as well as increasing company sales, there are complex legal pitfalls that come with this un-navigated territory. As companies make decisions to use social media to protect their brand or monitor activity related to their company or products, it is important to understand the potential legal implications of such engagement. There is significant increased risk with regard to civil liability that companies need to consider as they create social media strategies.

A. Negligence/Product Liability-

Some manufacturers mine social media to understand what people are posting about their products. If a manufacturer happens upon a post discussing a product being misused or misapplied, there is an issue whether the manufacturer's liability is increased now that it can be argued such misuse is foreseeable. In product liability actions, exposure is increased if a manufacturer can foresee the defective condition. Foreseeability is defined in Restatement (Third) of Torts as follows:

> *A person acts negligently if the person does not exercise reasonable care under the circumstances. Primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are the foreseeable likelihood that the person's conduct will result in harm, the foreseeable severity of any harm that may ensue, and the burden of precautions to eliminate or reduce the risk of harm.*

Courts have not addressed whether awareness of social media complaints give rise to "foreseeability" but the same standards apply for online activities. The bottom line is whether the manufacturer should have reasonably known that the product was dangerous.[1] It seems clear that if a manufacturer has actual knowledge from reviewing social media of complaints or product misuse, they will be found to have actual knowledge. But should a manufacturer be held responsible for constructive knowledge of social media complaints for which they "should have been aware"? The argument ought to be made that any company's products would all become cost prohibitive if employees had to be hired to cultivate comments from social media about the use or misuse of its products. The bottom line to keep in mind is that foreseeability is always a question of fact for the jury to determine. Certainly if an individual complaint goes "viral", there could be a determination of constructive knowledge, but for now, those watching ***Rob Dyrdek's Ridiculousness*** are probably safe.

B. Fraud/Misrepresentation- Unless it really is*: "The World's Greatest Cup of Coffee."*

[1] *Palsgraf v. Long Island R.R. Co.*, 248 N.Y. 339, 162 N.E. 99 (N.Y. 1928).

Companies need to be careful not to misrepresent their products or services or other facts related to their companies on social media sites. Fraudulent misrepresentations are defined as intentional misrepresentations of one or more material facts made by a person or business to another with knowledge that the representations are false. The misrepresentations must have been made for the purpose of inducing another party to act or refrain from acting. In civil lawsuits, the misrepresentation must have resulted in actual injury or damage. There can also be negligent misrepresentation.[2]

Misrepresentation is distinguishable from puffery, which is merely an exaggerated statement used to sell a product or a service. Puffery typically involves opinions, whereas misrepresentation relates to facts. In addition to common law fraud or misrepresentation claims, most states have consumer protection statutes that protect consumers from misrepresentation.

C. Defamation

Companies that post information on social media sites need to ensure that information is not defamatory. Defamation is the communication of a false statement that harms the reputation of an individual person, business or product. Attempts to get a leg up on competitors could lead to the posting of information that may not be accurate about another company's products or services.

D. IP Infringement

Companies have to be careful not to use third party trademarks or copyright works. It can be permissible as fair use to reference a company or its products or services on the internet, trademarks of others cannot be used to create a false impression of sponsorship, affiliation or endorsement. In addition, copyrighted works such as photographs, texts or videos should not be copied without authorization. A company should seek permission before using such information.[3]

E. Privacy Rights

Companies need to be careful not to post private information. For example, posting video or photographs without having the proper releases signed may violate publicity or privacy rights. In certain industries, such as healthcare, companies must ensure that they do not violate specific privacy regulations such as the Health Insurance Portability and Accountability Act ("HIPAA"). Any comment about a patient's condition on social media could violate HIPAA.

F. Regulatory Exposure

In this age of increased government regulation, greater transparency and omnipresent social media, consumer product manufacturers, importers, distributors, and retailers must be proactive to ensure regulatory compliance and to protect their brand by either setting the record straight or taking corrective action.

---

[2] *See* *http://www.ehow.com/info_8542087_elements-fraudulent-misrepresentation.html*. (last visited, January 12, 2016)

[3] http://www.infolawgroup.com/2011/06/articles/social-networking/the-legal-implications-of-social-networking-the-basics-part-one/

1. CPSC

The U.S. Consumer Product Safety Commission ("CPSC") has been among the most active government agencies in the last four years. Armed with greater power by way of amendments[4] to the Consumer Product Safety Act ("CPSA"), the CPSC continues to use all means available to it to encourage consumer products manufacturers to attain compliance with the CPSA and related regulations, and to sternly punish those who fail to do so. Among the measures the CPSC has utilized are increased filing of administrative lawsuits to ban products from the market, civil penalties that are assessed with greater frequency and in larger amounts, and civil penalties that include requirements that compliance programs be implemented or improved.

Social media has broadened the ways companies receive information about product issues so it is imperative that companies familiarize themselves with the rules and regulations applicable to their products in order to promote compliance and to effectively identify and make any required reports of any noncompliance. Section 15(b) of the CPSA establishes reporting requirements for consumer product manufacturers, distributors, and retailers. Each is charged with a duty to notify the CPSC *immediately* if it receives information that reasonably supports the conclusion that a product:

- fails to comply with a voluntary consumer product safety standard upon which the CPSA has relied under section 9 of the CPSA;
- fails to comply with an applicable consumer product safety rule;
- contains a defect that could create a substantial product hazard; or
- creates an unreasonable risk of serious injury or death to consumers.

The CPSC considers a company to have knowledge of product safety-related information when that information is received by an employee or official of the firm who may reasonably be expected to be capable of appreciating the significance of that information. 16 C.F.R. Sec. 1115.11.

Failure to report can result in significant penalties: $987,500 for Wooden Hammock Stands, $850,000 for Blenders, $400,000 for Baby Boat, etc.

In that regard, social media should be of critical import to all consumer manufacturers, distributors and retailers. Once someone identifies a substantial product hazard, whether through direct contact via social media with the company or through indirect contact that the company learns of, the company must react. Times are changing – it is no longer acceptable for companies to ignore social media, especially when many companies use social media for their own business purposes. Remember the standard is foreseeability – not whether the company receives the information but whether it could have reasonably discovered the information.

2. FDA

Certain rules dictate what information a company can relay to the public or its customers through the use of social media sites. For example, pharmaceutical companies must abide by rules promulgated by the Food & Drug Administration ("FDA") when providing statements to patients or doctors through warning labels, package inserts, written correspondence, or visits to a doctor's office

[4] The CPSA was amended by the Consumer Product Safety Improvement Act of 2008 ("CPSIA").

by a company's sales department—and this applies equally to promotional statements made on any online forum.[5]

A 2012 report by PricewaterhouseCoopers Coopers LLP indicated that one third of U.S. consumers use social media sites such as Facebook, Twitter, and YouTube for health-related matters. These include forums for seeking information on specific diseases, about medical treatment, and for communicating opinions about drugs and devices.[6] Companies must remember that any communication by a company outside these regulatory parameters may be used against the company as evidence that the company acted in violation of government regulations, leading to a potential cause-of-action under strict liability and negligence. For example, a company may have a blog or chat room where patients and/or doctors correspond with the company, and this direct communication may include off-the-cuff comments that contain language outside the parameters of information that the company is allowed to relay regarding its products (*i.e.*, off-label use).

III. The Ugly- When It Hits at Home- Social Media: The Means for Getting into Trouble for Employees and Employers Alike

Clearly, companies worldwide see social media as the new medium to reach customers. But those companies have employees, whose own use of social media can cause their employers both business and legal problems, including:

- Claims by coworkers against the company for harassment, negligent retention or supervision, or infliction of emotional distress[7]
- Trade secret disclosures
- Comments damaging the company's reputation and business interests[8]
- Defamation
- Intellectual property infringement
- Disclosure of private customer and client information
- Fraud
- Unfair competition claims
- Securities laws claims
- Privacy related torts

---

[5] *See Promotional Standards for Prescription Drugs* – 21 C.F.R. § 202.1.

[6] PricewaterhouseCoopers LLP, "Social media likes healthcare: From marketing to social business," available at http://www.pwc.com/us/en/health-industries/publications/health-care-social-media.html

[7] An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment claim created by a supervisor with immediate authority over the employee. *Burlington Industries, Inc. v. Ellerth*, 524 U.S. 742, 765 (1998). Employers may also be liable if it knows or has reason to know of work-related harassment occurring on social media. *See*, *e.g.*, *Faragher v. City of Boca Raton*, 524 U.S. 775, 779; Folkerson v. Circus Circus Enterprises, Inc., 107 F.3d 754, 756 (9th Cir. 1997); *Blakey v. Continental Airlines*, 2 F. Supp. 2d 598 (D.N.J. 1998); *Amira-Jabbar v. Travel Services, Inc.*, 726 F. Supp. 2d 77 (D. P. R. 2010)

[8] *E.g.*, Chrysler had a contract with a social media marketing firm, New Media Strategies, which managed its social media websites. In early March 2011, a tweet was posted on Chrysler Auto's Twitter account which stated "'I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to f***ing drive.'" The tweet was posted by a now former employee at New Media Strategies and was quickly removed from Twitter. However the next day, Chrysler announced that it would "'not renew its contract with New Media Strategies . . . for the remainder of 2011.'" *See* http://www.informationweek.com/internet/social-network/chrysler-addresses-twitter-foul-up/229300704.

- Violation of Non-Compete agreements;[9] and
- False endorsement and FTC Endorsement Guide issues[10]

A. Employers Monitoring Employees' Social Media Use: The Need for an Electronic Communications Policy

An employee may believe that his electronic communications at work are private, but that is not the case when his communications take place during work time using company-owned devices (cell phones or computers). However, an employer's ability to monitor and access an employee's electronic communications might only be as broad as the scope of its electronic communications policy and the reach of its computer systems.

The Fourth Amendment to the U.S. Constitution creates privacy rights for public sector employees, but private sector employees (except those in California)[11] have no constitution right to privacy. However, even private sector employees can assert common law privacy rights. When it comes to emerging technologies, however, the U.S. Supreme Court has urged caution when determining privacy expectations in communications made on electronic equipment owned by an employer. *See City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010). In *Quon*, the Court refrained from deciding whether an employee had a reasonable expectation of privacy in text messages sent and received on employer-provided devices, and disposed of the case on narrower grounds. In doing so, the Court warned that the judiciary "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." The Court further stressed in *Quon* that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

A well-drafted electronic communications policy will, in most cases, eliminate any reasonable expectation of privacy in employee communications sent or stored on company systems or servers. *See, e.g., Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) ("[the employee] had no right of privacy in the computer that [the employer] had lent him for use in the workplace . . . [Where an employer has] announced [a policy stating] that it could inspect the laptops that it furnished for the use of its employees, . . . this destroyed any reasonable expectation of privacy that [the employee] might have had and so scotches his claim."); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("[R]egardless of whether [the employee] subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [his employer] notified him that it would be overseeing his Internet use."); *Miller v. Blattner*, 676 F. Supp.2d 485, 497 (E.D. La. 2009) ("Where, as here, an employer has a rule prohibiting personal computer use and a published policy that emails on [its] computers were the property of [the company], an employee cannot reasonably expect privacy in [his or her] prohibited communications."); *Sims v. Lakeside School*, No. C06-1412(RSM), 2007 WL 2745367, *1 (W.D. Wash. Sept.

[9] *See*, *e.g.*, *Amway Global v. Woodward*, No. 09-12946, 2010 WL 3927661 (E.D. Mich. Sept. 30, 2010) (refusing to overturn arbitrator's award for, among other things, defendant's violation of a nonsolicitation agreement for posts on a blog); *TEKsystems, Inc. v. Hammernick*, No. 10-cv-00819-PJS-SRN (D. Minn. 2010) (alleging violations of non-compete, non-solicitation, and non-disclosure agreements when defendant contacted current contract employees via LinkedIn).

[10] In October 2009, the FTC updated its Guides Concerning the Use of Endorsements and Testimonials to include social media activities. *See* 16 C.F.R. § 1255. As a result, employees commenting on company products and services must now disclose company affiliation. Failure to do so could result in liability for an employer.

[11] *See Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 18, 865 P.2d 633, 642-43, 26 Cal. Rptr. 2d 834, 844 (Cal. 1994).

20, 2007) ("[W]here an employer indicates that it can inspect laptops that it furnished for use of its employees, the employee does not have a reasonable expectation of privacy over the employer-furnished laptop.").

The Supreme Court has recognized that different employers need different types of electronic communications policies. "Given the great variety of work environments, … the question whether an employee has a reasonable expectation of privacy must be addressed on a case by case basis." *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). "Because an employer's announced policies regarding the confidentiality and handling of email and other electronically stored information on company computers and servers are critically important to determining whether an employee has a reasonable expectation of privacy in such materials, the cases in this area tend to be highly fact-specific and the outcomes are largely determined by the particular policy language adopted by the employer." *In re Reserve Fund Securities and Derivative Litigation*, 275 F.R.D. 154, 160 (S.D.N.Y. 2011) (listing cases).

B. Employer Risks in Terminating Employees Because of Social Media Posts

Taking adverse action against an employee because of social media posts may trigger several federal and state employment statutes.

1. Off-Duty Conduct Laws

Employers should be generally aware that several states (California, New York, Colorado, and North Dakota) have passed statutes protecting employees in their "off duty conduct", recreational activities, and political practices.[12] Blogging or posting may perhaps be covered by these statutes.

2. The Digital "Water Cooler:" The Right to Bitch About Your Job.[13]

The National Labor Relations Act provides rights to employees to complain about the conditions of their employment. If an employee's internet posting represents an effort to organize a union or relates to a labor dispute between the employer and its employees, an employee could argue that any discipline relating to the postings constitutes an unfair labor practice. Specifically, the NLRA grants employees the right to "engage in other concerted activities for the purpose of mutual aid and protection."[14] The NLRA has been interpreted to protect non-union employees' concerted efforts to better the conditions of their employment.

For organizational speech to be protected it must be: 1) concerted; and 2) for mutual aid and protection. The National Labor Relations Board ("NLRB") and courts have arrived at varying definitions for "concerted" speech. Examples include: "organizational speech directed at only one other employee; speech that failed to actually produce any concerted group activity but appears to have had such activity as a primary goal, speech from employees who are merely spokespersons on matters of common concern, speech amounting to merely an implicit attempt to induce concerted action on the part of other employees, speech that is a logical outgrowth of previous group activity; and even completely

[12] *See*, Cavico, et al. at pp. 19-22.
[13] For a detailed discussion of this topic, *see generally*, Cavico, et al., at pp. 15-18; *see also* Davis, "Social Media Activity & the Workplace: Updating the Status of Social Media," 39 Ohio Northern University Law Review 359 (2012).
[14] *See* National Labor Relations Act, 29 U.S.C. §§ 157-158(a)(1)(2000).

independent expressive activity, not preceded by any group discussion and not characterized as a protest, as long as the activity implies a common goal to alter workplace conditions."[15]

In *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit recognized an employee's comments on his secure website as concerted speech. Konop's website bore bulletins critical of his employer, Hawaiian, its officers, and the incumbent union. The Ninth Circuit ruled that Hawaiian Airlines' discipline of a pilot who used his personal website to "vigorously criticize[]" the airline's management and labor concessions sought by the airline constituted protected union organizing activity. In so ruling, the Court rejected Hawaiian's arguments that the pilot lost this protection because his comments contained "malicious, defamatory and insulting material known to be false."[16]

The protection afforded by the NLRA is not absolute. Employees who engage in disloyal behavior or disparage the employer's customers or business activities are not protected by the NLRA. For instance, in *Endicott Interconnect Techs. v. NLRB*, where an employee posted his protests concerning recent layoffs and stated that his employer's recent layoff of 200 employees was causing the business to be "tanked," the D.C. Circuit reversed the NLRB's decision that the employee's resulting discharge constituted an unfair labor practice. The Court held that the employee's posting was so detrimentally disloyal that his discharge did not violate the NLRA. The Court reasoned that the employee's comments constituted "a sharp, public, disparaging attack upon the quality of the company's product and its business policies" at a "critical time" for the company, and were therefore unprotected by the NLRA.[17]

Final Thoughts: Some Recommendations for dealing with Social Media.

There is no escaping the new reality for every business in the world: "business as usual" for the foreseeable future will involve social media. While businesses have an amazing new set of tools with which to work to advertise their products and services, they are dealing with a Pandora's Box in terms of social media use by their employees. Social media presents new challenges to the employer. Fortunately, these are challenges that can be met head on and dealt with successfully.

[15] Andrew F. Hettinga, *Expanding NLRA Protection of employee organizational Blogs: Non-Discriminatory Access and the Forum-Based Disloyalty Exception*, 82 S. CHI. KENT L. REV. 997, 1001-02 (2007).
[16] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 872-73 (9th Cir. 2002).
[17] *Endicott Interconnect Techs. v. NLRB*, 453 F.3d 532 (D.C. Cir. 2006)