The Right and Responsibility of Social Media Monitoring

A Firestorm Insight Paper

07/23/14

A Firestorm Insights Paper
July 23, 2014

1000 Holcomb Woods Parkway | Suite 130 | Roswell, GA 30076 | 770-643-1114 | **Fax:** 1-800-418-9088
www.firestorm.com

Page Intentionally Left Blank

The Right and Responsibility of Social Media Monitoring

INTRODUCTION

Across the world, nearly one in four people have a social media account. This could be Facebook, Twitter, Instagram, Google+, Tumblr…the list continues. According to eMarketer, the number of social network users will increase from 1.47 billion in 2012 to 1.73 billion this year. That's an 18 percent increase in just two years.

A couple of years ago, while watching a livestream of President Obama's visit to Facebook, as the President walked in to the room, every single person raised their smartphone above their head. 'This is the new salute,' I thought. This is 'Social.'

—Karen Masullo, EVP of Social Media, Firestorm

We'll throw some more numbers at you; more than 1.1 billion Facebook users upload 350 million photos a day. In just one minute, more than 100 hours of video are uploaded to YouTube. During Hurricane Sandy, Instagram users posted 10 storm related images *per second*.

In addition, 64 percent of employees visit non-work related websites each day. This number increases to 86 percent following March Madness. More recently, the World Cup final blew through all previous social records: Facebook reported that 88 million (including 10.5 million in the U.S., 10 million in Brazil, over 7 million in Argentina, and 5 million in Germany) people had more than 280 million social interactions related to the final. And the match broke the record for the highest level of Facebook conversation for any single sporting event.

1.1 billion Facebook users upload 350 million photos a day

The final also set another social-media record: 618,725 tweets per minute on Twitter at the end of the match, exceeding the previous 580,166 tweets per minute during Germany's 7-1 squash of Brazil.

What does this mean? Essentially, employees today of all ages and skill levels spend a great deal of time on the Internet, including social media sites. As long as the surfing doesn't interfere with work-related tasks, it's not an issue, right? Wrong.

Not only can the use of social media during work hours be detrimental to your business, but so can off-the-clock Internet use.

There's a nation-wide debate regarding social media: Should companies monitor employee social media activities? When is the line of ethical and non-ethical crossed? But first, what exactly *is* social media monitoring?

Monitoring is the process that keeps you on top of what others are saying about your organization, brand and results. It alerts you to online customer requests, comments and when two-way communication is expected. Monitoring keeps you informed of relevant industry discussions, data and opportunities. It also positions you to track your competitors or learn what your employees are saying to one another about your organization and clients. Most important, it allows you to spot opportunities *and* risks and manage both in real or nearly-real time.

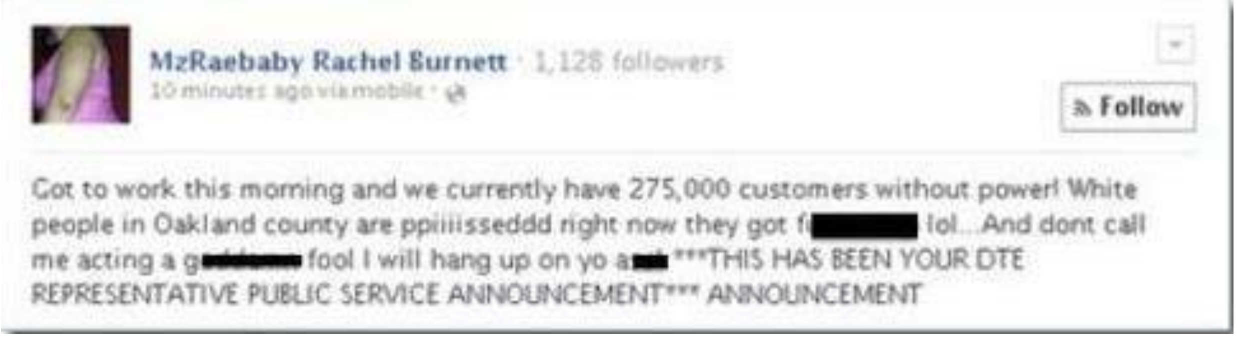
REAL-LIFE CASES

The number of cases of employees being fired because of online posting is astronomical. You may find numerous examples on the Firestorm Blog. Here are a few that stand out:

In 2009, Timothy DeLaGhetto took to Twitter to publicly complain about his work uniform at California Pizza Kitchen. The former server tweeted to corporate*, "black button ups are the lamest s**t ever!!!"* Corporate took noticed, figured out at which restaurant he was employed, and the rest was history. Making the most of the firing, DeLaGhetto then created a YouTube video entitled "Twitter Got Me Fired!!!" to explain to his fans (from his point-of-view) the termination. The video has more than 500,000 views.

In June of 2010, former Pittsburg Pirates' mascot, Andrew Kurtz, 24, was fired after voicing his opinion online. The former mascot posted, "*Coonelly extended the contracts of Russell and Huntington through the season. That means a 19-straight losing streak. Way to go Pirates."* It came shortly after the news of the team's choice to extend the contracts of two of its managers was released.

In 2013, A Detroit power company employee publicly insulted the company's customers on her own Facebook page. The post quickly resulted in her termination.


MzRaebaby Rachel Burnett · 1,128 followers
10 minutes ago via mobile ·

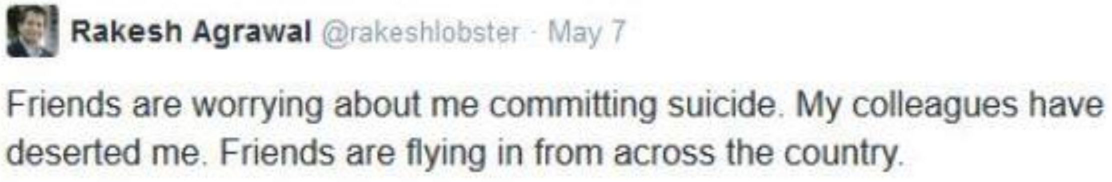
Got to work this morning and we currently have 275,000 customers without power! White people in Oakland county are ppiiiisseddd right now they got f[redacted] lol...And dont call me acting a g[redacted] fool I will hang up on yo a[redacted] ***THIS HAS BEEN YOUR DTE REPRESENTATIVE PUBLIC SERVICE ANNOUNCEMENT*** ANNOUNCEMENT

One tweet can terminate employment as seen in December of 2013. Former IAC director of communications, Justine Sacco, lost her job after tweeting *"Going to Africa. Hope I don't get AIDS. Just kidding. I'm White!"* To make matters worse, the PR executive boarded a 12-hour flight to South Africa just after tweeting. The hashtag #HasJustineLandedYet began trending during her flight. Upon arrival, Sacco deleted her social media accounts, but it was too late. She was quickly terminated because of the tweet.

Employees have lost jobs due to inappropriate social media behavior. But what happens when former employees take to social media *after* they have been terminated?

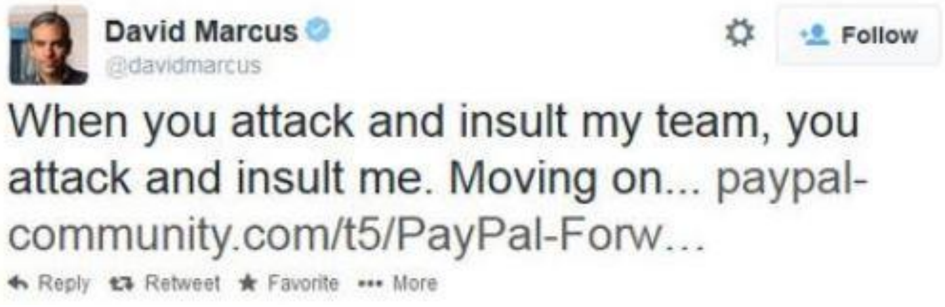
UK entertainment retailer HMV went viral while downsizing a total of 190 employees in early 2013. One of said employees had control over the company's social media and did not stay quiet during the termination. Tweets began rolling out stating: *"We're tweeting live from HR where we're all being fired! Exciting!!"* Another read, *"There are over 60 of us being fired at once! Mass execution of loyal employees who love the brand."* Directors of the company quickly took notice. The Twitter user "Poppy Rose" later took responsibility for the tweets. According to the former employee, *"Just to set something straight, I did not 'hijack' the hmv twitter account. I actually assumed sole responsibility of Twitter & Facebook over two years ago, as an intern. When asked (this afternoon), I gladly provided the password to head office."*

Most recently was the May 2014 Twitter meltdown of Rocky Agrawal. Agrawal took to social media to announce his resignation as Director of Strategy at PayPal, although PayPal implied he was terminated. He then continued to publicly insult Christina Smedley, Vice President of Global Communications. The tweets did not stop there. His rants sparked comments from PayPal President, David Marcus and former co-workers. Friends and family members of Agrawal went to the extent of calling the NYPD out of fear of his mental stability. The meltdown was very detailed and very public. Read Firestorm EVP of Social Media, Karen Masullo's, analysis of the disaster here.



Rakesh Agrawal @rakeshlobster · May 7

Friends are worrying about me committing suicide. My colleagues have deserted me. Friends are flying in from across the country.



David Marcus @davidmarcus

When you attack and insult my team, you attack and insult me. Moving on... paypal-community.com/t5/PayPal-Forw...

OPPOSING VIEWS

The number of people terminated for social media postings is on the rise. Even more so, employers are turning to the Internet during the hiring process. In a 2013 study from CareerBuilder, 39 percent of employers dig into potential candidate social profiles. Forty-three percent said they found something that made them hesitant to hire that candidate. At the same time, 19 percent said they found information that solidified the hiring decision of an individual. In a Wall Street Journal article, Nancy Flynn, founder and executive director of the ePolicy Institute, offered her opinion. *"Management has a right and* *responsibility to monitor how employees are using social media at all times."* Flynn further stated that like email, social networking records can be subpoenaed and used as evidence in court.

> In *Park W. Galleries, Inc. v. Hochman*, a court concluded that an individual could have been speaking on behalf of his employer, a gallery, when he posted allegedly defamatory statements on his blog. The court determined that there was sufficient evidence to support the existence of an agency relationship when the statement was made. The evidence cited by the court was a posting on the individual's LinkedIn profile. On the profile, the individual identified himself as a "Consultant/Writer at Park West Gallery."

In the article, Flynn described how serious social media postings can be when it comes to confidential information; *"Fourteen percent of employees admitted to emailing confidential company information to third parties; six sent customers' credit-card data and Social Security numbers; another six transmitted patients' electronic protected health information."*

Lewis Maltby, president of the National Workrights Institute, argues the opposite view. *"Employers don't need to practice wall-to-wall monitoring of employees' social media to protect their legitimate interests."* He states that companies only need to monitor when there is a solid reason to suspect employee wrongdoing. *"The vast majority of what employees do on the Internet has nothing to do with work, takes place during their private lives and is done on their personal computers."*

In light of the ever mounting regulatory, legal and financial pressures, the management of social media risk must be approached in your organization with three key components: a mature plan, a mature team and the flexibility to quickly adapt to or disregard rapid-launch and new technologies.

At Firestorm, we know there may be no warning sign to indicate a crisis is about to occur. By encouraging employee brand advocacy and participation in social interactions, and through training in how to do so appropriately, a broad spectrum of potential challenges may be addressed beforehand. This is the foundation of the Firestorm PREDICT.PLAN.PERFORM.® methodology. Your organization must be positioned to be ready to respond to a threat or incident before it occurs.

SOCIAL MEDIA MONITORING: WHAT YOU SHOULD KNOW

Employers continue to struggle with how to discourage social media postings that portray the employer in a negative light in a manner that is compliant with recent rulings.

These recent labor board and court rulings provide more guidance to employers on how to word their social media policies in order to be compliant with federal law;

What type of employee behavior can your social media policy legally address?

- Behavior that is offensive, that is not about working conditions or concerted activity;
- Personal venting that is not aimed at improving working conditions or wages;
- Inappropriate postings that include discriminatory remarks, harassment, and threats of violence or unlawful conduct.

Your social media policy cannot:

- Prohibit anything posted that is legal, while off-duty and not job related;
- Contain a blanket prohibition against employees posting things that 'damage the company' or 'any person's reputation';
- Contain a prohibition against offensive, abusive, disrespectful or inappropriate remarks (as this would include protected criticisms of the employer's labor policies or treatment of employees)
- Require employees or job applicants to provide their personal social network passwords.

Communication or content that is subject to disclosure is not altered by the fact that the content was delivered through social media channels. They are no different from other types of communication.

NASD Rule 3010:

- The obligations of an organization to keep records of communications made through social media depend on whether the content of the communication constitutes a business communication- even those conducted through personal devices.
  FINRA Regulator Notice 11-39, 08/2011
- Each organization must establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable federal securities laws and FINRA rules. As part of this responsibility, a registered principal must review prior to use any social media site that an associated person intends to employ for a business purpose.
- An organization should not include a link on its website to a third party site if there are any red flags that indicate the linked site contains false or misleading content.
- Organizations must adopt procedure to manage data feeds to their own websites.

> *Companies that have adopted social media without a clear monitoring plan are not truly using social media.*
> *-Jim Satterfield,*
> *Firestorm President*

Bottom line: Social Media policies must be thoughtfully worded using very specific language that puts the employee on notice of the detailed actions that are prohibited and serve as grounds for termination.

Any language that impacts an employee's right to engage in concerted activity, to improve working conditions or to seek mutual aid is prohibited and will violate federal law.

Companies need to be aware of what is being said online. It is more important, however, to train employees about social media use. Rather than focusing on resolving an issue that has already occurred, focus on preventing one from ever happening. The Firestorm PREDICT.PLAN.PERFORM strategy must be followed. Predict what crises could occur on social media, plan for them to happen and if they do occur, take the necessary actions to resolve the issue.

Employees and management must understand that their personal accounts not only reflect themselves, but also the company. It is imperative that a social media policy that is sensitive to corporate culture is in place and effectively communicated with *everyone* in the organization.

CREATING BRAND ADVOCATES

Every employee is a brand advocate. You must teach them to be a trusted one.

Professional social media networking site, LinkedIn, offers five pieces of advice for creating brand advocates.

1. Encourage your employees to use social media. No one wants to feel like their employer is watching over their shoulder, waiting to catch them sharing something on social media that shouldn't be shared. You need to create a culture within your company that is supportive of employee engagement on social media.
2. Communicate frequently. Your employees want to hear from you because communication is one of the top factors that can create brand advocates. When you have information you want to share, make sure you are sharing it on multiple channels, multiple times. For example, not everyone is going to read an email, join a company-wide meeting, and check their intranet, but chances are they will do one of those things. Be very transparent about what people can share and what needs to stay internal. If your employees feel like they're "in-the-know" and that you trust them, they will act appropriately.
3. Make it easy. Give your employees content to share; it's as simple as that. Direct your employees to follow your company on social media sites and share out your updates with their networks. Also, when you share news with your employees (typically via email), include some pre-formulated status updates and suggest that they use them when posting on social media. This will save time for them and give employees the extra nudge to share. Want your employees to have a consistent voice across social media? Provide them with a suggested sentence or two about your company that they can add to their social media profiles. This makes it very easy for them to represent their employer when networking with other people.
4. Train your employees. Not everyone feels comfortable with social media, and that's ok. However, you can help your employees feel more at ease and more confident about social media if you provide training. No one (that I know of) does this better than Dell. Through their Social Media and Community University, they have trained thousands of their employees who now are brand ambassadors on Dell's behalf... And even if you don't have the resources for formal training program, hold brown bag lunch 'n' learns, work it into your new hire orientation, and send tips to your employees. Even a little training and guidance can go a long way.
5. Customize your game plan. Not every employee is the same, and different types of people require different tactics in order to turn them into brand advocates. But how do you know what types of employees and social media users you have at your company? How can you identify them? Weber Shandwick recently published a great whitepaper entitled "Employees Rising: Seizing the Opportunity in Employee Activism" that identifies six types of employees (ProActivists, PreActivists, HyperActives, ReActivists, Detractors, InActives) and provides insight into how to approach each type.

THE BOTTOM LINE OF THE ISSUE

The greatest *risk* for your organization regarding social media is in not understanding that **everyone** in your organization who leverages social media **owns social media.** Everyone in your organization must be trained on the organization’s internal policies and regulations that apply. Moreover, everyone’s activity must be carefully monitored, and where necessary, retained and indexed as **organizational leadership will be held accountable.**

"There is a significant lack of understanding by social media users that monitoring must be equal in scale to adoption, and that monitoring goes beyond marketing analysis; it can be used to track brand and company threat trends, competitor information, employee use and misuse, brand detractor attacks, and a variety of new product development and service enhancement initiatives via customer engagement. Companies that have adopted social media without a clear monitoring plan are not truly using social media."

— James W. Satterfield, President & CEO, Firestorm as quoted in ContinuityInsights

Firestorm believes that preventing a crisis from ever occurring is essential. In order to avoid a social media crisis, a plan must be created, brand advocates must be formed and monitoring must be established.

Let us know if you have questions. We can help.

FIRESTORM®

PREDICT. PLAN. PERFORM.

770.643.1114

info@firestorm.com

ABOUT FIRESTORM

FIRESTORM® transforms crisis into value. The FIRESTORM PREDICT.PLAN.PERFORM.® methodology combines C-Suite level consulting, dynamic software solutions, and proven crisis management expertise to empower clients to create resilient organizations. FIRESTORM is a nationally recognized leader in Crisis Management, Continuity Planning, Critical Decision Support, Crisis Response, Crisis Communications, Crisis Public Relations, and Consequence Management.

We are the Crisis Coach® (800) 321-2219

Firestorm services help clients protect their employees, assets, revenues, reputation and, ultimately, the value to all stakeholders. Firestorm services are designed to include emphasis on the human component in every crisis. The Firestorm core philosophy is 'Every Crisis is a Human Crisis', and this philosophy is embedded into all recommendations and implementations, to ensure organizations focus on people, processes, and procedures.

THE FIRESTORM® SELF-ASSESSMENT

Firestorm encourages private sector entities to use the newest PS Prep certification framework as a means of measuring the preparedness of their organizations, as well as that of their key suppliers/vendors.

Firestorm Self-Assessment tools provide insight to an organization's current level of preparedness, and provide a roadmap for the development of an up-to-date business continuity program that will empower organizations to mitigate threats and vulnerabilities.

FIRESTORM'S PREDICT.PLAN.PERFORM.® PROCESS

As experts in vulnerability analysis, risk mitigation, planning, and crisis management, Firestorm offers organizations of every size immediate access to its expertise and guidance in planning and preparing for any type of emergency along with plan enhancement/development, including business continuity, crisis communications, crisis management, security, workplace violence, and communicable illnesses.

Firestorm's guidance allows its clients to complete plans, address emerging issues, and have resources available as needed. The client directs the project plan, timing, and resource level required. Firestorm manages the process and produces the deliverables. Firestorm will complete the work necessary to bring planning to the level of best practices.

Proper disaster planning requires that companies PREDICT the vulnerability, PLAN the response, and PERFORM when the event occurs. The PREDICT phase classifies the critical vulnerabilities, identifies key emergency personnel, ascertains critical decision processes, analyzes gaps, identifies infrastructure and supply chain needs, and defines communications requirements. The PLAN phase develops the strategy, constructs the plan, and involves the appropriate personnel to assure their buy-in and commitment. The PERFORM phase establishes protocols for implementation, community involvement, communications, test exercises, audits, reviews, updates, and compliance.