

SOCIAL MEDIA DURING DISASTER RESPONSE

A LAWYER'S PERSPECTIVE

BY JOE MCMENAMIN

Social media hold tremendous potential for facilitating disaster recovery. In the recent Haitian earthquake, for example, Twitter posts enabled the State Department to initiate a set of steps that led to finding and saving an individual trapped under rubble from a collapsed building, and alerted NBC that landing restrictions designed to facilitate military air traffic had prevented a plane chartered by Doctors Without Borders from delivering badly-needed medical supplies. By bringing the problem to the attention of the military, NBC helped solve it.

Examples abound from around the world. Major oil companies are using Twitter to post hurricane updates. Filipinos used social media to coordinate rescue efforts during the recent Typhoon Ondoy. During the Mumbai terror-



ist attack, tweets identified hospitals in need of blood. On the other hand, the terrorists, who themselves were skilled in use of social media, eluded pursuers and prolonged the violence by monitoring the activities of the police and the military. In February, 2009, Twitter provided updates and alerts on bush fires in Australia. That same year, after the Iranian government blocked conventional communications, Iranian demonstrators were able to communicate via social media.

Other examples are closer to home. Within 90 minutes of the first deaths at Virginia Tech in April, 2007, Wikipedia

featured an article accurately describing the events. A mere 20 minutes later, Facebook users had set up a group called "I'm OK at VT," allowing students and staff to assure friends and loved ones that they were safe. During the more recent shootings at the University of Alabama, students used Twitter to complain in real time that the University's alert system had failed to notify them of the attack. Campus police, focused as they were on trying to limit the carnage, were criticized for failing to notify students and others. One wonders whether social media might not have been helpful here as they were at Virginia Tech.

CONTINUED ON PAGE 22



Photo courtesy of Marvin Neuman/FEMA

The Los Angeles Fire Department posts alerts about major fires and road closures. For snow emergencies, the City of Minneapolis has created a Facebook page providing information on closed streets and winter parking restrictions. The Washington (State) Department of Transportation uses social media to report traffic alerts, route changes for ferry vessels and so forth.

In emergencies, information is critical. These examples demonstrate that social media provide unprecedented communication capabilities. The potential for benefit is clear. Despite these many benefits, however, organizations should be alert to risks, notably including legal ones. The rapidity that gives these media their potential for benefit also gives them their power to inflict harm.

Consider confidential corporate information. A disaster does not change the sensitivity of trade secrets, intellectual property, or insider information. Once the information is disseminated, during an emergency or not, the damage is done.

Consider the risk of fraud liability. The Securities and Exchange Commission takes the position that a company is responsible for statements made by it or

on its behalf and that the law's anti-fraud provisions apply to such statements. There is no exception for information conveyed on YouTube or LinkedIn. Companies may not be able to avoid liability by having employees speak through social media only as individuals. Nor can companies avoid liability by requiring users, as a condition of participation in a blog, to waive antifraud protections under the securities laws. On the other hand, SEC has said that a company is not responsible for third-party statements, even on company-sponsored websites. The site sponsor need not monitor its site or correct misstatements made by strangers. As of this writing, however, FDA has made no similar statement with respect to sites controlled by pharmaceutical, medical device, or biotechnology companies.

Privacy law applicable to new media is unsettled. In *City of Ontario (California) v. Quon*, 08-1332, the Supreme Court will decide, perhaps by June, whether police officers enjoy a "reasonable expectation of privacy" in sexually explicit text messages they allegedly transmitted on department-issued SWAT team pagers. The officers had signed a document

warning them that the department had the right to monitor their communications using official media, but had not explicitly stated that text messages were included in the materials that could be searched. The case illustrates the need to state the organization's privacy policy fully and clearly.

Harassment claims can be based upon online statements; they need not be focused on sex. References to race, religion, age, or national origin may all give rise to harassment claims. In fact, the plaintiff need not even be the person harassed but could be anyone claiming to be affected by the offensive conduct. Nor need the harasser bear any special relationship to the plaintiff, and a claim can be brought even if no economic harm can be shown. The new media allow offensive statements to be disseminated more rapidly than ever before.

Of particular pertinence to business continuity professionals, the media may themselves be a source of business disruption. As suggested above, carelessness in handling confidential data, or posting inaccurate or offensive statements, can give rise to a wide array of legal problems. But the social media may themselves create an emergency. An unhappy airline passenger, claiming that his musical instrument had been ruined by baggage handlers, aired his complaint via a YouTube video that has now been seen millions of times. The damage to the company, though reputational and not physical, is every bit as real, and serious, as any caused by fire or flood.

The good news is that organizations can also harness the power of the internet to rectify, or at least ameliorate, problems such as these. When a cable technician visited a customer's residence to replace a faulty modem, he was put on hold with the home office for so long that he fell asleep on the customer's couch. When after three weeks the problem remained unresolved, the customer posted a video on YouTube capturing the technician asleep on the job. Once again, millions of visitors have watched this video online. In this instance, however, the company developed programs to turn problems around quickly and

now follows up with the customer to be sure any such problem is resolved.

In another example, employees of a pizza chain videoed themselves adulterating food intended for human consumption and then mounted the video on YouTube. Once again, millions of viewers saw the video before it was pulled down. The company suffered significant financial loss as well as damage to its well-established brand reputation. The company president, however, quickly harnessed YouTube himself, issuing a heartfelt and highly effective apology. He provided reassurance to customers, shareholders, employees, and the public at large, noting that the restaurant in question was being scrubbed down stem to stern, and that the misconduct was wholly at variance with the company's philosophy and track record. The president pointed out that his company employs well over 100,000 individuals across the country and that the local franchise owner had been severely hurt. He also told viewers that the perpetrators had not only been discharged, but were facing felony criminal prosecution. The apology was so well done that the pizza chain not only survived but actually by some measures raised its stature in the eyes of consumers.

Social media, then, must be recognized as powerful engines for both good and ill. It follows that organizations should develop rules for the use of social media by employees, not only during disasters, but at all times. One option is to bar outright any such use on company time. Assuming the company wishes to utilize or permit employees to use social media, however, it should establish clear guidelines for information to be posted about the company and limit those authorized to blog, post or tweet on its behalf. Specific rules will vary from organization to organization, but several principles may be of general utility. Information conveyed via social media should be limited to non-controversial public or non-material data. If tweets are used, the 140-character limitation makes it difficult, if not impossible, to provide a balanced presentation. A link to more complete statements else-

where on the internet might solve that problem. Someone should monitor data regularly and amend statements that are out of date, out of line, or simply incorrect. Media policy should be updated regularly. Policies must be enforced not only against employees, but also against management –for reasons not only of equity but also of effectiveness.

The company's policies should make plain that it can and will monitor communications made with its equipment or network or appearing to have originated with the company; that misusing social media is grounds for discipline, including termination; and that it will take-down any defamatory, infringing or otherwise unacceptable content posted through its media. Before disciplining an employee for something he did online, however, the company should conduct a careful investigation to determine the facts and seek advice of counsel. The company should prohibit:

- disclosure of confidential, trade secret or proprietary information
- using company email addresses to register for social media sites
- posting false information about the company or its employees, customers or affiliates
- appearing in uniform or
- speaking for the company without express authorization.

The organization can also require adherence to its non-harassment and non-discrimination policies and demand that an employee whose personal blog identifies his employer post a disclaimer prominently on his blog or webpage. Companies should ask employees to keep company logos or trademarks off such sites, and train supervisors and managers how to handle social media issues, including those arising from use of the media themselves. The organization should develop a plan of prompt action to combat a social media disaster.

The company should also create a policy for use of these media specifically in disaster recovery and business continuity contexts, coordinating with the approach taken by local authorities. The company should select its own designated communicator and a back-up or

two. It could develop message templates that can be edited as needed, listing, for example, evacuation centers and contact data for key personnel. Mock emergency response trials should be conducted regularly. In an actual disaster, posts must be monitored for accuracy. The company must be prepared to make corrections quickly, specifically including posts attacking it. Finally, social media can be used to rebuild after the emergency ends.

Social media offer a uniquely rapid and powerful way to disseminate information – good and bad, accurate and inaccurate.

Conclusion

Social media offer a uniquely rapid and powerful way to disseminate information – good and bad, accurate and inaccurate. In deciding whether to use them to communicate, organizations must consider both the benefits and the risks. Among the latter are legal issues, including some thorny ones. The law applicable to these media is evolving, and organizations electing to use them would be wise to follow that evolution and to be governed accordingly.

ABOUT THE AUTHOR

Joseph P. McMenamin was a university-trained internist and a practicing emergency physician before being admitted to the bar. He is a partner with McGuireWoods and an Associate Professor in the Department of Legal Medicine at the Medical College of Virginia in Richmond. He can be reached at jmcmenamin@mcguirewoods.com , or (804) 775-1015.

**WANT HELP?
LOOKING FOR RESOURCES?**
Visit the online guide at
www.disaster-resource.com