Legal Risks in Social Media Use by Nonprofits

Kenneth E. Liu, Gammon & Grange, P.C.

As the world has seen in the grassroots revolutions of 2011, online social media can be powerful tools for social change. Nonprofits large and small are increasingly taking advantage of such tools to advance their causes. But as with all new societal advances, social media also pose many risks if not used properly. As your nonprofit organization grows its social media presence, be sure to take steps to avoid the many potential legal traps in the online world, which should include formulating a social media policy to guide your employees on acceptable online behavior. Below are some tips and pointers on avoiding legal troubles in the use of social media.

1. Direct your employees not to post anything that they would not want to see on the front page of The New York Times or to hear on the witness stand.

Even if you use a pseudonym online, there are ways that the public, including reporters, can discover who you are, as three young staff of Congressman Rick Larsen of Washington state found out the hard way. In December 2011, these three legislative aides apparently did not have enough to do, so they made a pact to get drunk at their office every day for a month. If that alone was not bad enough, they were foolish enough also to tweet about their daily drunken adventures. Although they did so under anonymous Twitter names, a Washington news blogger discovered their identities, and suddenly their embarrassing tweets were exposed to the world. Generally, information posted in social media can also be used as evidence in a court of law. And even what you delete from social networks can get you into trouble. In 2011, a lawyer in Virginia told his client to remove several photos from his Facebook account for fear that they would prejudice his wrongful death case brought after his wife's fatal automobile accident. Unfortunately for him and his client, a judge chastised the lawyer for treating social media data differently from other forms of evidence, which litigants are prohibited from deleting once litigation is imminent. The judge ordered the lawyer to pay $522,000 for instructing his client to delete the photos, and the client to pay $180,000 for doing so.

Remember also that any data posted online is not only available worldwide, it can potentially remain forever. Even when privacy settings are restricted or a page is password-protected, there are still ways to retrieve data using cyber forensic tools, even after the data is "deleted."

2. Actions taken by an organization's employees can be held against the organization.

Under the legal doctrine of respondeat superior, employers can be held liable for the activities of employees. In the social media world, the line between one's personal life and professional life is becoming increasingly blurred. This ambiguity increases the risk of an organization being held liable for the online posts of its employees.

Many employees of charities and advocacy groups are passionate about their work, so they naturally speak out publicly on issues relating to their field. If an employee posts an offending statement against another organization on Facebook or another social network, the statement could be attributed to the employer, even if the employee posted on his or her own personal
account. The risk is higher if the employee's profile clearly states his or her organization, his or her title as a senior staffer, and includes the logo of the organization.

Organizations can minimize such risk by requiring that personal postings and blogs of employees that relate to the employer's field be carefully distinguished from the employer, such as by including a disclaimer stating that the views and opinions expressed do not represent those of the employer. Such disclaimers alone do not automatically insulate an employer from liability, but may be helpful as one factor in the liability equation. In addition, employers should prohibit employees from using the organization's logo on personal accounts.

3. If you're not allowed to do it in the "real world," you're probably not allowed to do it in a virtual world.

Although social media might often feel like a separate world, it is still subject to the laws of the real world. The context might be different, but the obligations to which a nonprofit is subject in the real world generally also apply online. Social media may be more casual, but that does not excuse illegal activity. Below are some sample legal issues implicated by social media use.

**Intellectual Property (IP).** Nonprofits typically have two primary forms of intellectual property (IP): trademarks and copyright. Trademarks are words or designs that identify the source of a particular product or service, including organization and program names, logos, and slogans. Copyrighted works include any content expressed in a tangible medium, including web sites, books, reports, videos, music, photos, and graphics, etc.

Organizations need to prevent their employees from misusing IP in two ways: (1) misusing the organization's own IP in a way that jeopardizes the organization's rights, and (2) infringing on the IP rights of others. An employee can misuse his or her employer's IP by, for instance, using the organization's trademarks without authorization to misrepresent the organization's position on issues, to provide false information, or to make defamatory remarks. This can happen if an employee uses the organization's logo on the employee's personal blog or other social media account.

An employee can violate others' IP by, for instance, copying and using others' trademarks or copyrighted works on social media without a proper license. Just because something is available on the Internet does not mean that it is free for anyone to copy. Unauthorized copying can result in bad public relations as well as significant liability.

**Hostile Work Environment, Harassment, and Discrimination Claims.** According to a 2011 Associated Press-MTV poll, 59% of young adults have experienced some form of harassment through social or online media. While most employers recognize that they have a duty to maintain a workplace atmosphere free of illegal harassment, they often don't realize that they may face liability when employees use social media to make discriminatory statements, racial slurs, or sexual innuendos directed at co-workers. Recently, a California jury awarded $1.6 million to a juvenile corrections officer with a severely deformed hand after co-workers referred to him as "rat claw" and "one handed commander" in an unofficial blog.
**Political campaign activity.** 501(c)(3) organizations are prohibited from participating in any political campaign on behalf of, or in opposition to, any candidate for elective public office. Violating this prohibition may result in excise taxes and possibly even revocation of tax-exempt status. Organizations can unwittingly violate this prohibition if their employees speak out in favor of, or in opposition to, political candidates through social media and their statements are attributed to the organization.

**Charitable solicitations.** Thirty-nine states require some type of registration for charities soliciting funds within their jurisdiction. Certain states are more aggressive than others about whether online requests for funds constitute solicitation. In some states, the mere existence of a "Donate Now" button can trigger the registration requirement. Use of social media to raise funds can also trigger the requirement, especially if the fundraising is directed toward people known to reside in a particular state. If your organization solicits funds online or through social media, be sure to comply with charitable solicitation laws in the appropriate jurisdictions. Failure to comply can result in significant fines.

**Improper Disclosure of Confidential or Other Protected Information.** Organizations must take care to prevent disclosure of confidential or proprietary information through social media. For instance, if an employee blogs about a donor or a constituent your organization has served, he must be careful not to reveal any personally identifiable information without authorization.

These and many other legal risks can be minimized by taking certain precautions, such as the following.

4. **Implement a social media policy to govern use of social media by employees.**

The foregoing concerns certainly do not warrant a ban on employee use of social media, not necessarily even within the office. Social media is now thoroughly ingrained in the fabric of our society. If your nonprofit wants to get its message out and engage its donors and constituents, you not only want to permit employees to use social media, you may want to actively encourage it, depending on your organization's field and mission. However, it is crucial that organizations act prudently in guiding and training their employees in using social media appropriately.

One key step in protecting your organization is to have a written policy that provides guidance on what your employees can and cannot do in social media, both in their role as employees and in their personal use. Because every organization has a unique mission, purpose, and culture, each organization should develop a policy that addresses its own needs. For instance, groups working on sensitive matters may find it necessary to be more strict, while others that have a broader educational or advocacy mission may want to be more lenient in letting employees get the message out. Therefore, it is important to tailor a policy to the needs and goals of your organization. It may be prudent also to include certain provisions governing social media use in employee contracts.

5. **Instruct employees to use only official organization social media accounts for conducting business.**
Employees' use of personal social media accounts for official organizational business can not only cause confusion between employees' professional and personal online identities, it can also create problems when employees leave the organization. For instance, the organization can lose valuable history, content, and contacts if it can no longer access accounts used by a former employee. Also, organizations can end up in disputes with former employees about ownership of accounts and data. To minimize these concerns, require employees to conduct official business only through the organization's social media accounts, not through personal ones, and insist that the organization's accounts should not be used for personal affairs.

Social media have become an invaluable technology for advancing the cause of nonprofit organizations. Whether your organization is just beginning to leverage this powerful tool or has already mastered its potential, be sure to consider the legal risks and take adequate steps to minimize them.

Kenneth Liu (kel@gg-law.com) is an Intellectual Property & Internet attorney with Gammon & Grange, P.C. (www.gg-law.com), a law firm serving charities and other nonprofit organizations throughout the United States. His practice involves advising nonprofits on trademark selection, registration, and protection; negotiation of license agreements; and litigation/dispute resolution. He also counsels clients on Internet, domain name, and copyright issues; website legal risk management and audits; and social media policies. Additionally, Mr. Liu helps to establish nonprofit corporations, obtain federal tax exemption recognition, and advise on compliance with federal and state regulations. He received a B.A. from the University of Virginia in 1993 and a J.D. from Cornell Law School in 1997.

Source for article: