

We are happy to provide you our publication for nonprofit risk managers, as part of our service to you. The titles in the contents section link directly to their articles. If you need to change the email address to which this is sent, please [contact us](#). Be sure to include your name, organization and address. You also are welcome to call us at 800.222.8920 for assistance.

In this issue...

[They can't say that! Can they?](#)

[Coming soon...social media in insurance underwriting](#)

[Making the most of your volunteer application](#)

[For insurance industry, 2011 is a year of the "cat"](#)

[CIMA service team for VIS® members](#)

[VIS® Commitment](#)

They can't say that! Can they?

An emerging area of employment practices liability is on display in recent decisions by the National Labor Relations Board (NLRB) regarding what constitutes "protected concerted activity" by employees using social media sites such as Facebook. If employers ignore the issue, or react in the wrong way, it can be damaging to the organization and to relationships among employers, employees and volunteers.

In September, an NLRB administrative law judge ruled in favor of five employees who had been fired by a Buffalo, NY nonprofit organization. One of the employees had posted a comment on Facebook complaining about another employee, and about working conditions. The other four employees had commented on that posting. All this occurred outside of working hours, and the employees used their own computers. The employer fired the five on the basis that their comments amounted to bullying and harassment of the employee targeted in the comments, in violation of the organization's stated policy. Judge Arthur Amchan disagreed, ruling that the comments were within the scope of "protected concerted activity" because they dealt with terms and conditions of employment. The judge ordered the employees reinstated.

Over 100 cases have been brought before the NLRB, following a 2010 ruling in favor of an ambulance company employee in Connecticut who used a vulgar term to describe his employer, on the employee's Facebook page. Acting board counsel Lafe Solomon wrote in a recent report, "Most of the social media policies that we've been presented are very, very overbroad. They say you can't disparage or criticize the company in any way on social media, and that is not true under the law."

In not all cases has the NLRB ruled that the statements made in social media are protected activity; for example, the board ruled in favor of Walmart when an employee made a general complaint about management "tyranny" and was fired. The "individual gripe," in which the employee did not attempt to solve a problem either by complaining to management or by discussing it with other employees, is not protected activity, Solomon wrote. The board also ruled in favor of a car dealership that fired a salesman for posting photos of, and comments about, a vehicle accident that occurred at the dealership next door. But the NLRB has made clear that employees can communicate with coworkers about jobs and working conditions in any forum they choose, including social media.

Even given the parameters of Solomon's report, employers may find it difficult to determine what is protected activity and what is not. Michael Eastman, labor law policy director at the U. S. Chamber of Commerce, told the Associated Press, "Employers are struggling to figure out what the right policies are and what they should do when these cases arise;" for example, when an employee goes "over the top" in his or her criticism about a supervisor or working conditions. "Where will the board draw the line between concerted activity and an employer's legitimate non-disparagement policy?"

Attorneys Andrew Matzkin and Tyrone Thomas of the Mintz Levin law firm pointed out in a recent newsletter, "Employers should be aware that the National Labor Relations Act protects both organized and non-organized employees and...protects the rights of all employees (whether or not unionized) to discuss and engage in ...concerted activity related to their working conditions."

Social media policy for the workplace – a few suggestions

- State that your social media policy is concurrent with your Internet usage policy, and any policies concerning privacy, nondisclosure, ethics, etc. If you maintain your policies in electronic form, link your social-media policy to any related ones. Your Internet usage policy should confirm the fact that you can monitor any messages sent or received within your organization's own communication systems. Get the same point across, in whatever way suits your style, with respect to using your systems for access to social media. (Although with smart phones, employees don't need your systems to engage in social media.)
- With your social media policy and any other policies, require employees to acknowledge that they have read them, understand them, and agree to them as a condition

of employment. It is a good opportunity to remind employees that you are an “at will” employer (unless you have employment contracts or collective bargaining agreements that limit termination options.) Employment “at will” means you can terminate employment at any time, for any reason that is not discriminatory, with or without notice.

- Let employees know that, if they publish anything about your organization, they are to include the fact that they are employed there, and that their views are entirely their own; e.g., “What I write reflects my personal views, and not necessarily those of my employer.” No logos or trademarks may be displayed, because doing so creates the impression that the employee is writing on behalf of the organization.
- Emphasize the risks of online publishing, including the risk that confidential information might be disclosed. If information hasn’t been released by the organization itself, it should not be released by any employee. Prohibit the release of any audio or video recordings made at the workplace, or photos taken there. Expertise for which clients pay the organization shouldn’t be shared with the public. If in doubt, employees should check with their supervisors, or other person you designate, before publishing. If they receive inquiries from the media (including bloggers), they should refer the inquiry to the organization’s official media contact person.
- Employees are liable for what they publish. They can be sued for libel, plagiarism, copyright infringement, invasion of privacy and other offenses. Let them know that if they publish words or images that are embarrassing or otherwise harmful to your organization, they may be disciplined to the full extent of the law. (Even as the NLRB cases discussed above illustrate that the law is evolving.) Make it your policy that employees be respectful in what they say about the organization, other employees, clients and everyone else. This is a point to make in the hiring process and employee orientation, too. Set your people’s expectations.
- Be careful not to disclose anything that would allow someone’s personal information to be compromised. Be wary of “phishing” emails, and malicious software. Review the privacy settings on your social-networking site to minimize the risk of this kind of invasion. Be careful not to link to sites that might be infected.
- Some organizations include additional guidance to help employees have a positive influence in whatever social media channels they operate. For example, your policy might point out the importance of checking facts before publishing, attributing information to the proper source, and making sure that opinion is presented as exactly that, and not as fact. You also might encourage employees to “read before they write” in social-media environments, so they understand views that already have been expressed; to be the first to correct their own mistakes; and to be constructive and respectful in correcting others. Anyone publishing online also should indicate how he or she can be contacted. Because these points might not be obvious to all, you can do your employees a favor by pointing them out.

Sample policy

The Louisiana Society For the Prevention of Cruelty to Animals has a detailed social media policy. Following is an excerpt related to the use of social networks, and used with the organization's permission. It is provided here for guidance only, as every organization's needs are different.

Online social networks include sites like Facebook, MySpace, Twitter, and LinkedIn (and many, many more). There have been a number of questions regarding proper "etiquette" on these sites. While there are no official rules when it comes to the following, these are our recommendations.

- Use Facebook and MySpace (and similar sites) as your personal network. If you don't want to 'friend' coworkers, volunteers, competitors, or clients, don't feel pressured to.
- Use LinkedIn as your professional network for adding work-related colleagues.
- If you feel uncomfortable with adding a contact, don't add him or her. These might include former employees, competitors, volunteers or clients.

The following are guidelines we request you abide by while you are employed with LA/SPCA:

1. Do not access your personal social network on company time unless to post to LA/SPCA Facebook or Twitter account.
2. Be smart about what you publish. Once you put something out there, it can be difficult to retract.
3. Do not forward any email from your LA/SPCA account that is not work related. This includes chain emails, calls for action against legislation, personal pleas to adopt a pet, etc. Use a personal email address (not your la-spca.org address) as your primary means of identification. Just as you would not use LA/SPCA stationery for a letter to the editor with your personal views, do not use your LA/SPCA email address for personal views.

Resources

National Labor Relations Board – www.nlr.gov

Privacy issues

Law firm Morrison & Foerster maintains a [Privacy Library](#) that provides links to privacy laws, regulations, reports, multilateral agreements and government authorities for more than 90 countries around the world, including the United States.

Media Law Resource Center – www.medialaw.org

Monitoring what is being said about any topic (including your organization) in social media -- a few resources among many:

Technorati – www.technorati.com

BlogPulse – www.blogpulse.com

WordPress – www.wordpress.com

Google Alerts – www.google.com/alerts

Twittorati– www.twittorati.com

Coming soon...social media in insurance underwriting

For some time, insurance companies have been monitoring social media to detect fraudulent claims. Payments have been stopped when workers' compensation claimants were inspired to post, for example, a photo on Facebook that shows them waterskiing, participating in a 10K run, or some other activity that defied the physical limitations of their supposed work-related injury or illness. Now, the Boston-based research firm Celent has published "Using Social Data In Claims and Underwriting," which predicts that social media will be used increasingly on the underwriting side of the insurance business; i.e., determining the nature and extent of a risk before a policy is issued or renewed, or the price of the insurance is determined.

Just as credit reports, criminal and motor vehicle records and other publicly available data are used already in underwriting, insurance companies now have tools such as "social graphing," a connecting of the dots that taps social media to determine a purchaser's business or personal relationships. According to Celent, those relationships might allow underwriters to infer risks that an insurance application itself would not disclose. Predictive modeling software programs also are advancing rapidly, and can be combined with social graphing to provide underwriters information they can consider when evaluating risk.

Of course, privacy issues arise when technology allows an insurance company or anyone else to gather information such as this. The Celent report notes that insurance companies might begin seeking the customer's or prospect's permission to do that, perhaps in the form of an opt-in -- or (more likely) an opt-out. So it pays to read the fine print in those privacy notices, and think about your interests, regarding the information you are willing to share.

Making the most of your volunteer application

One risk that goes with volunteer involvement is that the volunteer will not feel that his or her talents are being used, and will leave the organization. "Volunteer Management Practices and Retention of Volunteers," a study for the Urban Institute by Dr. Mark Hager and Dr. Jeffrey

Brudney, found that volunteer recognition – not just awards, but also recognition of talents and interests – is a key element in retention. (Other key elements include training opportunities, and having volunteers actively involved in recruiting new volunteers.)

Thomas McKee, president and owner of www.volunteerpower.com, contributed an article to the September 2010 issue of *VIS Connections* in which he describes the importance of allowing today's volunteer to feel empowered, and how to make that happen. (To view that issue, go to www.cimaworld.com and click the "Periodicals" link.)

Are you using your volunteer application to identify the volunteer's talents and interests, and match that information with the most appropriate assignment (or even a new assignment)? Each organization is different in terms of useful information to collect, but consider simple questions such as these, which are taken from the application of one of the organizations participating in our Volunteers Insurance Service program:

- What is your education level (multiple choices, all the way through Ph.D degree.)
- What special skills or interests do you have?
- Why are you interested in volunteering?

The application also invites the volunteer to list the types of assignments, among the choices given, that would interest him or her most, and asks about previous volunteer experience, preferred hours, and any medical conditions or physical limitations that might affect the ability to carry out certain assignments.

Beyond the questions designed to match volunteer interests and assignments, the application also asks for three references, requires information about any criminal convictions, and asks if the applicant agrees to a criminal background check (because the organization deals with vulnerable clients).

For insurance industry, 2011 is a year of the "cat"

Throughout 2011, we have seen televised coverage of tornadoes, a hurricane, wildfires, flooding, parched farmland, and even a rare East Coast earthquake in the U. S. If there seems to have been an unusually high number of natural catastrophes – or "cats," in insurance industry lingo – you are right. And hurricane season doesn't end officially until November 30.

According to the Insurance Information Institute, 2011 already is the sixth most expensive year on record in the U. S. for "cat" claims payments, including:

Hurricane Irene – Between \$2 billion and \$4.5 billion once all claims are processed, according to catastrophe modeling firm Risk Management Solutions. That estimate does not include flooding of properties for which flood insurance had not been purchased through the National Flood Insurance Program. (More information about flood insurance is available at www.floodsmart.gov.)

East/Central Texas wildfires -- \$100 million in insured losses, according to the Insurance Council of Texas. Some 25,000 acres were burned, and 500 homes destroyed, primarily in Bastrop County.

MidAtlantic earthquake – About \$100 million in insured losses from the 5.9 magnitude quake that occurred on August 23, according to Impact Forecasting.

Tornadoes in southern U. S. – The April and May tornadoes caused some \$12.5 billion in insured losses, according to Swiss Re.

In all, according to the Insurance Information Institute, U. S. insurers paid about \$25 billion in claims from natural disasters from January through September. The number of declared federal disasters also is a record this year – 86 declarations to date, breaking the one-year-old record of 81 declarations.

As devastating as all these events were for those affected, they do not approach the magnitude of Hurricane Katrina's insured losses in 2005 (\$45 billion in 2010 dollars) or the terrorist attacks of September 11, 2001 (\$40 billion in 2010 dollars).

Insurers also have paid some \$70 billion in claims related to the earthquake/tsunami in Japan and the earthquake in New Zealand this year, according to Swiss Re.

“I just like to hold it.”

In British Columbia, where use of handheld cell phones while driving is illegal, police conducted a crackdown in September on all “distracted driving,” including cell phone use. Over 3,500 tickets were issued. In addition to collecting tidy revenue for the province, the officers also collected a number of excuses from drivers. The Insurance Corporation of British Columbia, a Canadian auto insurer, released the top ten:

1. This is a bogus law.
2. It was my boss on the phone – I had to answer it.
3. I wasn't using it – I just like to hold it.
4. Sorry officer, I didn't see you trying to pull me over because I was on my phone.
5. But it was an emergency call to my wedding planner.
6. My Bluetooth died.
7. Driver: I'm using my speakerphone. Police officer: No, you're holding your phone in one hand and steering with the other.

8. I'm not driving; I was stopped at a red light.
9. I wasn't talking, I was checking my messages.
10. I was just checking the time.

“It’s evident that there are still a lot of drivers who don’t realize that distracted driving can have tragic consequences,” said Shirley Bond, Minister of Public Safety and Solicitor General. “Every time we get behind the wheel, we have peoples’ lives in our hands – whether they’re the lives of our passengers, other drivers, cyclists or pedestrians. We need to stop making excuses and adopt new driving habits.”

New York enacted the first U. S. law banning use of handheld cell phones while driving, in 2001. Since then a number of states and local jurisdictions have followed suit, or at least banned texting while driving, an even more dangerous practice than using a cell phone. But it is a tough slog; a survey by State Farm in November 2010 found that 74 percent of respondents made or received calls at least once a week while driving.

CIMA service team for VIS® members

Volunteer insurance:

[Victoria W. Brooks](#), Account Executive

[Joan R. Wankmiller](#), Account Executive

Directors and officers liability:

[Aaron Jones](#), Account Executive

[Laurie S. Coleman](#), Senior Vice President

Toll-free: 800.468.4200

We are always happy to serve our members. Please let us know, any time we can be of help!

VIS® Commitment

Volunteers Insurance Service is committed to providing its members a complete resource for the nonprofit organization’s risk management needs. Our services include:

- Publishing *VIS® Connections* as one of our information resources for members;

- Maintaining for members' use a library of information relating to management of risks in the nonprofit organization;
- Researching available and appropriate insurance relating to volunteer activities;
- Designing and administering insurance programs, and compiling underwriting information;
- Providing consultation on risk management issues at no additional charge to our members, via a toll-free line (800.468.4200);
- Assisting members, on request, with matters relating to insurance.

Insurance and administrative services are provided to VIS® and its members by The CIMA Companies, Inc. and/or one of its affiliated companies.

VIS®'s Articles of Incorporation, Financial Information, and a list of the members of VIS®'s Board of Directors are available to VIS® Members upon request.

CIMA licensing information

The following licensing information is being provided in order to comply with state governmental regulations:

Volunteers Insurance Service Association, Inc. is a risk purchasing group formed and operating pursuant to the Liability Risk Retention Act of 1986 (15 USC 3901 et seq.)

Notice to Texas clients: The insurer for the purchasing group may not be subject to all the insurance laws and regulations of your state. The insurance insolvency guaranty fund may not be available to the purchasing group.

Notice to California clients: License #0B01377 and #0A06046, CIMA Companies Insurance Services

Notice to Minnesota clients: License #009285 and #07544084, The CIMA Companies, Inc.

CIMA, one of its subsidiary companies and/or an authorized individual is licensed in all jurisdictions. Please contact CIMA at 800.468.4200 if you would like information about our licenses.