

Toronto / Washington DC / Brussels  
[www.nymity.com](http://www.nymity.com)



**Philip Gordon**

Shareholder  
Littler Mendelson, P.C.

### Top 'Dirty Dozen +' Tips to Consider When Developing Your Web 2.0 Policies: Part I - Tips 1-6

Using Web 2.0 tools and social networking in a company setting can build a brand or destroy it in an instant. It's that quick. It is much like a coin toss. One side is opportunity and the other danger.

In our two-part interview, Philip Gordon of Littler Mendelson, P.C, highlights one dozen challenges to manage in order to have the opportunity to reap some of the benefits of Web 2.0.

Phil chairs Littler's Privacy and Data Protection Practice Group. Littler is the largest U.S.-based law firm that represents only management in employment and labor law matters. Phil has counselled hundreds of businesses on updating their policies to address new technologies, including social media. He also is the principle author of Littler's blog focusing on workplace privacy, [www.workplaceprivacycounsel.com](http://www.workplaceprivacycounsel.com).

**Nymity: First and foremost, what are the 'opportunities' that await companies that successfully manage their Web 2.0 environment with their employees, clients, contractors, business partners, and vendors, globally? What are the big ROIs to be gained?**

**Gordon:** Given the newness of the medium, the ROI from online resources is difficult to quantify, but the opportunities from Web 2.0, i.e., any form of interactive communication over the Internet, such as social media, abound.

In 2009, 80% of Chief Marketing Officers reported that product suggestions and stories from customers through social media shaped products and services. Best Buy's Chief Marketing Officer, Barry Judge, commented that what he is attempting to achieve with social media for Best Buy is to talk with customers - not at them, as Best Buy did with traditional mass media like TV, radio, newspapers and magazines. In other words, social media is not just about communicating externally but using the technology and platforms to connect an organization with its customers.

There also are opportunities to use social networking to connect employees and harness ideas internally. IBM, for example, has approximately 17,000 internal blogs which connect more than 100,000 employees. Within these blogs, employees exchange ideas, engage in conversations and even do a little self-promotion of their projects.

Another excellent opportunity created by social networking is the ability to better recruit new employees. Microsoft, for example, has embraced LinkedIn as a recruitment tool. Ernst & Young's Facebook site includes job opportunities for students as well as seasoned professionals along with pictures and videos of employee life in and out of the Ernst & Young offices. These posts provide context for prospective candidates that they would otherwise not be able to get. In addition, social media can vastly expand an applicant pool. One Tweet about a new position, made with appropriate hash tags, can send a job listing to tens of thousands of potential applicants in minutes.

Companies should realize that the opportunities for a large ROI utilizing Web 2.0 and other online resources are there. These opportunities can be harnessed once companies determine how to best utilize the technology to fit within their corporate culture and become comfortable with their online presence.

**Nymity: Tip 1: Online Background Checks: What are the risks? What are practices that should be curtailed? How can a company gain the benefits of the tools, and minimize those risks?**

**Gordon:** Online resources can provide a wealth of information about job candidates that would not otherwise be available to an employer through traditional means, such as an application, interview, and reference check. However, online background checks pose a range of risks that are not present when vetting applicants by traditional means. Many of these risks are not obvious.

For example, employers can now obtain a criminal history report at certain Web sites simply by entering an applicant's name or e-mail address. These Web sites typically do not hold themselves out as background check companies and, therefore, do not warn users that they are likely consumer reporting agencies regulated by the federal Fair Credit Reporting Act (FCRA). The FCRA permits employers to obtain a background check report on a job applicant from consumer reporting agencies only after notice to and consent by the applicant. In addition, the FCRA requires any employer that relies in whole or in part on such a report to reject an applicant to provide a pre-adverse action notice to the applicant, wait at least five days, then provide an adverse action notice. Employers can unwittingly fail to provide these procedural protections and, concomitantly, violate the FCRA because they do not realize that the Act applies to these online searches. This problem is particularly acute because employees conducting job interviews can access these Web sites without their employer's knowledge and may consider the results of the search when evaluating the applicant.

Another hidden risk involves access to an applicant's restricted social media presence. As more users adjust their privacy settings to "Friends Only" for Facebook or an equivalent setting for other social media sites, employers are finding it more difficult to glean information from social networking sites. Some employers might be tempted to use false pretences to bypass these restrictions, for example, by sending a bogus friend or connection request in the hope that the applicant will accept it. The federal Stored Communications Act (SCA) makes it unlawful to gain unauthorized access to electronic communications stored at a third-party communications provider. Several cases, including Crispin v. Christian Audigier, Inc., Pietrylo v. Hillstone Restaurant Group, and Konop v. Hawaiian Airlines, would support the position that the Act applies to posts on a restricted social media page. Another case, Theofel v. Fary-Jones, would support the position that the use of false pretences to gain access to such sites would constitute unauthorized access in violation of the SCA. Employers should note that the Act is a criminal statute with civil remedies, so violations could have severe repercussions.

The Genetic Information Non-Discrimination Act of 2008 (GINA) creates yet another hidden risk. GINA generally prohibits employers from acquiring "genetic information" about job applicants and employees. The Act broadly defines genetic information to include the manifestation of a disease or disorder in a family member, whether or not genetic in nature. While GINA's prohibition against employers acquiring genetic information does not encompass publicly accessible information, that exception does not apply to restricted Web sites. Consequently, if an employer gains access to a restricted social media page, whether by false pretences or with the applicant's consent, the employer could discover "genetic information" about the applicant given that it is not uncommon for social media users to post information about a family member's health condition.

Genetic information is not the only type of potentially problematic information that an employer might find posted on an applicant's social media site. Social media postings can reveal other information about an applicant that an employer might not learn through traditional means and upon which an employer cannot properly rely when making a hiring decision. An applicant, by way of illustration, might post information revealing that she is protected under the Americans with Disabilities Act, such as that she survived childhood leukemia or has a serious eating disorder, or that she is transgender, which many employers do not realize is a protected characteristic under many state or local laws.

Putting aside these legal risks, there are practical risks as well. The objective of the vetting process should be to hire the best talent for a particular position. Decision makers should be using relevant and reliable information. However, information posted on social

media sites often can be irrelevant or unreliable, and mere exposure to such information may taint a decision maker and prevent him or her from hiring the best talent for the position.

Employers can take several steps to mitigate these risks. First, online background checks should be integrated into an organization's FCRA compliance procedures, and all such checks should be conducted only through employer-sanctioned channels. Individual managers or interviewers should not be conducting rogue background checks. Second, the individuals who conduct the checks should be provided with guidelines on the type of information that may be provided to decision makers. Doing so will screen decision makers from information upon which they cannot lawfully rely. Finally, employers should give applicants the opportunity to explain any adverse information found on a social media site before reaching a final decision. The applicant's explanation may demonstrate that the information is false or cannot fairly be linked to the applicant. Even if the information is true and the applicant's responsibility, the applicant's explanation may demonstrate her maturity or her unfitness for the position sought.

**Nymity: Tip 2: Customer-Facing Company Sites: Such sites and other customer facing tools and techniques can build a brand over night. How does a company avoid the issues and gain the brand lifting benefits?**

**Gordon:** For many businesses, Web 2.0 has changed the nature of corporate communication. Previously, most businesses tightly controlled the channels through which the business communicated with the public and tightly restricted the group of employees authorized to use those channels. Many businesses that have embraced Web 2.0 as a means of communicating with their current and prospective customers have decentralized their public relations efforts, permitting more employees to communicate through a wider variety of channels. Some national retailers, for example, have a social media presence for each store and a group of employees within each store who are authorized to communicate on the organization's behalf.

Business leaders should keep in mind two fundamental points when deciding how to incorporate customer-facing social media into an organization's business strategy. First, there is no one-size-fits-all solution; each business needs to develop its own plan based on a range of factors, such as its corporate culture, the nature of its products and services, the profile of its customer base, and the abilities of its workforce. Second, if the business decides to permit employees who are not professional communicators to speak for the business on a company-sponsored site, the business should strongly consider providing communications guidelines for those who will be representing the company in social media. The organization also should implement a structure that will ensure proper training of employees and effective oversight of the business's social media presence.

The training and oversight should be aimed at ensuring that social media channels are used effectively and that related risks are minimized. Employers, for example, should encourage employees to post content that will be interesting to, and useful for, existing and prospective customers. Employees responsible for posting content should timely and fully respond to questions from their audience. Employees with subject matter expertise should be the ones to respond or should be consulted by those who will respond. Employees never should pick a fight with a customer and should know to seek assistance from public relations professionals when confronted with negative comments. Employees always should provide truthful information and promptly admit and correct any mistakes.

Training should focus not only on providing guidelines for effective use of social media but also on identifying and mitigating the most significant risks. Employees need to be reminded that all company policies as well as the company's code of conduct apply to social media interactions at company-sponsored sites. Businesses should focus particular attention on their policies aimed at protecting trade secrets. While most employees would not purposely reveal corporate trade secrets, employees might disclose a new product launch or recent financial success not realizing that the information is a trade secret. Another potential legal pitfall is an employee's failure to adequately disclose his or her affiliation with the employer when posting information that could be construed by readers as an endorsement of the business's products or services. Last year, the Federal Trade Commission issued guidelines that explain that an endorsement of a company's product posted on the Internet by a company employee without adequate disclosure of the employee's affiliation with the company could constitute an unfair and deceptive trade practice and subject the employer/company to fines and other penalties.

Effective oversight of employee's social media activity on company-sponsored sites has several different layers. The employees or categories of employees authorized to post should be carefully selected. These employees should be required to complete training that will provide effective guidance on how best to use social media to advance the business's interests while identifying the risks described above and explaining how they should be avoided. Employers should provide a referral source whom employees can consult with any questions. Finally, the business should actively monitor its sponsored sites to ensure that employees are complying with all guidelines and policies and to react promptly when a problem arises.

**Nymity: Tip 3: Individual Employee Sites for Business Purposes: Who "owns" these sites, such as LinkedIn contacts and Facebook fan pages? Must an employee establish a new account for their work with a company? What are the best practices in these situations?**

**Gordon:** "Ownership" of social media content created by employees in the ordinary course of business for purposes of advancing the employer's business interests has not yet been addressed by U.S. courts. The crux of the matter is that employees' work product is being stored on the servers of a third-party service provider rather than on corporate document management servers. Under the federal Stored Communications Act, a provider of electronic communications services to the public, such as an Internet Service Provider (ISP) or the host of a social media site, is prohibited from disclosing communications stored on the service's servers without the consent of the sender or of the recipient. That means, as a practical matter, that an employer could lose control over social media content created by employees for work purposes when the employee refuses to provide log-in credentials and refuses to consent to the employer's accessing content stored at the employee's social media site.

Employers can avoid this issue by requiring that employees agree in writing effectively to cede control over their work-related social media content to the employer as a condition of employment. Some of the key terms of such an agreement would include the employee's agreement to the following: (a) not to use any personal account to conduct company business; (b) to use a corporate e-mail address to open any work-related account; (c) that any such account is being opened for the employer's benefit; (d) to provide the employer with the log-in credentials for the account; (e) not to change the log-in credentials without providing the new credentials to the employer; (f) that the employee consents to the employer's accessing the account at any time; (g) to abide by all company policies as well as the corporate code of conduct when using the account to conduct company business; and (h) that the employer has the right to terminate the account upon termination of the employment relationship. While no court has yet opined on the enforceability of such an agreement, an employer who has one in place will be much better positioned in litigation seeking to prevent an employee from using the account's content for the benefit of a competitor.

**Nymity: Tip 4: Internal Company-Sponsored Sites: What is special about these that require policy statements or recommendations? Can these sites really be a problem?**

**Gordon:** Internal company-sponsored sites can provide an efficient means for employees to collaborate, especially for global employers spread across many time zones. Because these sites typically will be housed on the employer's own servers, or the employer will be the subscriber on the contract with the service provider, internal company-sponsored sites do not raise the same challenging issues that arise when employees use third-party social media sites for business purposes. Still, since the medium is new and the employer will have difficulty disclaiming vicarious liability for misconduct on an internal site, employers should guide employees on how to conduct themselves when using an internal social media platform.

Most of the guidelines will follow those that I described in response to your question about customer-facing sites that a business sponsors; however, some guidelines are unique to this medium. For example, employees need to be reminded of the more subtle principle of need-to-know as opposed to flat out prohibition against disclosure of trade secrets. More specifically, employees should not assume that just because access to the internal site is limited to the organization's workforce, that everyone with access to the site is authorized to review any information that might be posted.

For global employers, cultural sensitivity is another important issue. Words or images that might not offend U.S.-based employees could be highly offensive to employees with different mores and customs. Employees should be sensitized to these cross-cultural differences.

Controlling union solicitations is another critical issue. Employers do not want their internal social media platform to be converted into a union-organizing tool. Under a decision known as Register Guard, issued by the National Labor Relations Board (NLRB) in December 2007 during the final days of Republican control of the Board, employers can restrict use of their corporate e-mail system for solicitations in a way that incidentally prohibits solicitations for unions as long as the employer enforces the policy in a manner that does not discriminate against labor activity. An employer can, for example, prohibit any solicitation for a political cause, religious group, or membership organization (which would include unions) as long as the employer enforces the prohibition in a non-discriminatory manner. Critically, however, the NLRB's current chairperson dissented in Register Guard, and the NLRB's Acting General Counsel has announced that he is looking for cases that could be used to reverse that decision. Employers should watch for new developments in this area.

As with company-sponsored, customer-facing sites, employers should actively monitor any internal corporate social media platform. One advantage of monitoring an internal site, as opposed to a customer-facing site, is that the employer does not have to worry about being subjected to public scrutiny (or obloquy) for removing content from an internal site.

**Nymity Tip 5: Employees Off-Duty Social Media Activity. We've discussed social media activity for work purposes, what about employees' off-duty social media conduct. What are the risks there and how should employers address them?**

**Gordon:** Given the public nature of social media and the fact that employees can badly damage their employer's image or brand with a social media post that "goes viral," employers should strongly consider issuing guidelines for off-duty social media posts that discuss work-related matters or which prominently identify the employee's affiliation with the employer. According to a 2011 study by the Society of Corporate Compliance and Ethics (SCCE) and the Health Care Compliance Association (HCCA), more than 30% of employers have implemented a policy governing off-duty social media use.

Such a policy should focus in particular on off-duty conduct that could be severely damaging to the employer's business reputation or subject the employer to legal liability. Examples include disclosure of trade secrets, disparagement of the employer's products or services or the products or services of a competitor, endorsements that do not adequately identify the source, and unauthorized posting of images or personal information of customers (or patients) or co-workers.

One question that all employers confront is whether to permit or prohibit the use of corporate electronic resources for social media activity. Employers' most significant concerns in this regard typically are loss of productivity and exposing the corporate computer network to malicious software. Some employers take the view, however, that employees always will find a way to waste time, so why not earn some good will by permitting the workforce to use the corporate Internet access for social media activity. There is no right answer to this question. The decision to allow employees to use corporate resources to engage in social media may depend on the specific social media Web site being accessed. According to the SCCE/HAAC study, 47% of employers permit employees to access LinkedIn at work, while only 32% of employers allow access to Twitter and Facebook.

**Nymity: Tip 6: Disciplining Employees Based On Off-Duty Social Media Activity: There seems to be much confusion over when employers can discipline employees for their off-duty social media activity. What are the key risks to avoid? What are the best practices that can be adopted to avoid what types of risks?**

**Gordon:** In November 2010, the National Labor Relations Board (NLRB) turned this issue into a very hot topic. Then, the Board filed an unfair labor practices charge against an ambulance service, AMR, after AMR allegedly terminated an employee based on her social media activity. According to the NLRB's complaint, AMR denied the employee's request for union representation made after her supervisor asked her to prepare an investigative report in response to a customer complaint about her job performance. The employee then posted disparaging comments about her supervisor, including referring to him as a "17" (AMR's code for a psychiatric

patient), on her restricted Facebook page. Co-workers who were Facebook friends expressed support and also posted negative comments about the supervisor. AMR got wind of the posts and terminated the employee, in part, for violating its social media policy which prohibited employees from disparaging their supervisors.

The NLRB claimed that AMR's termination of the employee's employment violated her right to engage in "protected concerted activity" under the National Labor Relations Act (NLRA). The term protected concerted activity generally includes communications with co-workers about wages, hours, or other terms and conditions of employment. Importantly, the NLRA protects employees from infringement of their right to engage in protected concerted activity regardless of whether the workers at issue are represented by a union.

Even though the AMR case settled before trial and resulted in no published decision, the NLRB drew substantial attention to the scope of an employer's ability to discipline employees for their off-duty social media activity by issuing a press release when the complaint was filed and when the case settled. Since then several unions have filed unfair labor practice charges against employers who disciplined employees for work-related, off-duty social media activity. In addition, the Board has kept the issue in the spotlight through public statements by high-ranking officials.

Although substantial NLRB precedent addresses the concept of protected concerted activity, no published decision to date has addressed that concept in the context of social media. Consequently, employers face substantial uncertainty at this time. How an employer confronts that uncertainty in terms of the content of its social media policy turns on a range of factors, such as whether the employer is unionized and the aggressiveness of the union(s), whether the employer's corporate profile makes it more or less likely that the employer will attract the Board's attention, the degree of risk tolerated by the employer's corporate culture, and the likelihood that employees will disparage management in their off-duty social media posts.

Employers looking to significantly reduce risk could simply remove broad anti-disparagement language from their social media policy as well as other language that could be construed to infringe employees' right to engage in protected concerted activity. Employers who are less risk averse could consider adding a disclaimer to their social media policy which emphasizes that the employer will not apply the policy in a manner that interferes with employees' rights under the NLRA. Employers should note, however, that the NLRB has not yet addressed whether a disclaimer would suffice, let alone what that disclaimer should say.

While the NLRA imposes the most significant potential limitations on disciplining an employee based upon off-duty social media activity, employers should be aware of other laws. Four states – California, Colorado, New York and North Dakota — generally prohibit employers from taking adverse action based upon an employee's lawful off-duty conduct. Connecticut, for example, prohibits private employers from taking adverse action against an employee for speech involving a matter of public concern that would be protected by the First Amendment were the employee employed by a government agency. More than two dozen states prohibit discipline based on particular forms of lawful off-duty conduct, such as political activity or the consumption of a lawful product (e.g., tobacco or alcohol). These statutes could come into play if the employee's social media content violates company policy but also reflects support for a particular political candidate or contains images of the employee consuming a lawful product.

Finally, employers always should keep anti-discrimination statutes in mind. To the extent social media activity reveals information that might justify a termination as well as information which reveals that an employee is in a protected class, or genetic information about an employee, the employer should analyze whether the employee might have a legitimate basis to allege that the employer relied on prohibited information for its employment decision.