SOCIAL MEDIA: NEW OPPORTUNITIES AND HEADACHES[1]

By Leslie G. Bottomly
July 2011

This article addresses some of the legal issues that arise from employee use of social media, including a discussion of whether employers should view their applicants' Facebook page or Google results as part of the candidate screening process; whether an employee can be fired because of their off-duty on-line postings; whether on-line statements can trigger whistleblower and/or concerted activity (National Labor Relations Act) protections; and the implications of Federal Trade Commission regulations on an employee's on-line comments about the company's products. Finally, development of an appropriate social media employment policy is discussed. These materials focus on private, non-union workplaces. Additional constraints and considerations apply in governmental and union workplaces.

A. Vetting Job Applicants On Line

According to a 2009 study conducted by Harris Interactive for CareerBuilder.com, 45 percent of responding employers were using social networks to screen job candidates.[2] There are advantages and disadvantages to doing so.

1. Advantages to Reviewing Social Media

Recruiting, hiring, and training a new employee is hard work and takes significant amount of time, money and energy. Employers want to avoid mistakes in hiring. As a result, they often a desire to find out as much as possible about a candidate before taking the leap and offering them the job. Access to social media sources may help an employer obtain the "big picture" about an applicant—does the online information fit with what you know from other sources of information? Does the applicant exercise good judgment in online disclosures? What is his or her reputation online? Does the applicant spend a great deal of time disparaging his former employers or updating their online information during work hours? According to the survey referenced above:

> More than half of the employers who participated in the survey said that provocative photos were the biggest factor contributing to a decision not

---

1 This memorandum contains a summary of information obtained from laws, regulations, court cases, administrative rulings, and legal publications and should not be viewed or relied upon as legal advice. Ater Wynne LLP urges readers of this memorandum to consult legal counsel regarding specific legal issues and factual circumstances.

2 Jenna Wortham, *More Employers Use Social Networks to Check Out Applicants*, http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/.

> to hire a potential employee, while 44 percent of employers pinpointed references to drinking and drug use as red flags. Other warning signs included bad-mouthing of previous employers and colleagues and poor online communication skills.[3]

Checking an applicant's online activity is prevalent in industries that require their employees to be knowledgeable of, and use, social networking as part of their work. This is why, for example, some companies advertise jobs primarily through Twitter—they want Twitter-savvy employees. The use of social media sources, such as looking up an applicant's blog, Twitter feed, or Facebook page (if done directly by the employer rather than an outside vendor), generally does not require disclosure or authorization by the applicant under the Fair Credit Reporting Act. In addition, unlike reference or background checking firms, which charge a fee, reviewing online profiles is often free.

2. Disadvantages of Examining Social Media

Employers are struggling with how to articulate fair and uniform standards by which to evaluate online information about job candidates. In addition, employers that view personal web pages risk exposure to information about an applicant's protected class. It would not be unusual to learn from a candidate's blog or Facebook page, for example, that the candidate is a minority, has a particular religious faith, is planning to have children, has a disability, has filed workers' compensation claims, or is a union activist. Even if the employer does not base its hiring decision on these facts, which would be illegal, simply learning such information renders the employer more vulnerable to discrimination claims. An employer who has learned about the candidate by viewing his or her online profile cannot "plead ignorance" about the individual's status or protected activities.

Another concern is privacy. Absent the applicant's consent, looking at password-protected information that the applicant has affirmatively attempted to restrict may constitute an invasion of privacy and likely violates the terms and conditions of most social networking sites.[4] Some employers require a candidate to access their Facebook or MySpace site in the employer's presence so that the site can be reviewed with the candidate. The City of Bozeman, Montana, attracted negative publicity when it was revealed that it had for years required job candidates to reveal their password and login information for social media sites.[5]

3. Insulating the Decision Maker

An employer may take steps to screen the hiring decision maker from protected class information embedded in social media. Employers can do this by outsourcing the task to a third

---

[3] Id.

[4] See, e.g., Hilton Collins, Montana City Asks Job Applicants for Social Media Passwords, Draws Controversy, http://www.govtech.com/gt/732085.

[5] Declan McCullagh, *Want A Job? Hand Over Your E-Mail Login*, http://www.cbsnews.com/stories/2009/06/18/national/main5096450.shtml; Molly McDonough, Town Requires Job Seekers to Reveal Social Media Passwords, http://www.abajournal.com/news/article/town_requires_job_seekers_to_reveal_social_media_passwords.

party with instructions to screen out protected class information (or instructions to just provide information on limited criteria (*e.g.*, evidence of illegal activity). As an alternative, the employer could designate a "neutral" individual internally to research the candidate's social networking information, screen out protected class information, and provide the remaining data to the decision maker. Employers should instruct the neutral party to withhold any and all information pertaining to an individual's protected class when reporting back to the decision maker. If this screening function is outsourced to a vendor, the employer should be aware that the Fair Credit Reporting Act likely requires it to provide notice and obtain written consent from the applicant.[6]

Employers that use social networking as a screening tool should consider developing a policy on this practice in order to ensure consistent treatment and respond to discrimination claims. Such a policy should articulate the legitimate business reasons for the inquiry, describe the criteria that will be considered, and should articulate information that will be disregarded if learned during the process. Others have suggested that any screening of social networking sites be conducted only after a conditional job offer has been made. This would presumably allow an employer to rely upon information learned in the review of social media as a reason to withdraw an offer, and combat discrimination claims based on factors the employer was aware of when the offer was made (before the applicant's online information was accessed).

B. Can You Fire Someone Because of Their Online Conduct?

Given the proliferation of online activity, it is no surprise that employers sometimes discover objectionable conduct or communications by their employees on Twitter, blog postings, or Facebook pages. An individual may express dissatisfaction with their work, their pay, their manager or their coworkers. An individual may exhibit unprofessional photographs or reference getting drunk or being hung over at work, or may disclose confidential employer information. For private (non-governmental) and non-union employers who have engaged employees on an at-will basis, the default assumption is that an employee can be terminated for any reason or no reason and certainly for disparaging the employer or its products, for goofing off at work, for being drunk at work, and similar activities employees frequently tweet or blog about.[7] For example, Virgin Atlantic Airways fired 13 flight attendants after they posted jokes on Facebook about passengers and faulty airplane engines.[8] Employees of public entities may have free speech, due process, and greater privacy protections.[9] Finally, collective bargaining agreements and private individual employment contracts may specifically define "cause" for termination and outline the types of off-duty conduct that can result in disciplinary action.

---

6 15 USC § 1681, *et seq.*, 16 CFR Part 601.

7 *See generally*, Gerard P. Panaro, *The HR Troubleshooter, Can You Fire Employees for 'Blogging'?*, 13 No.3 HR Advisor: Legal & Practical Guidance 6 (May/June 2007).

8 *Id*.

9 If the employee is working for a public employer, first amendment and due process protections must be considered. *See e.g., Richerson v. Beckon*, 2008 WL 833076 (WD Wa), *aff'd* 337 Fed. Appx. 637 (9th Cir 2009) (plaintiff alleged she was reassigned in retaliation for the exercise of her First Amendment free speech rights exercised through a blog regarding her observations as an employee of the school district; summary judgment granted to her employer—noting that blogger's speech disrupted co-worker relations and interfered with her duties).

Legal Risks

Although there is a presumption of at-will employment for private Oregon employers, which will often allow employers to terminate an employee because of the employee's objectionable online activity, there are exceptions to this general rule. For example, an employer may not interfere with an employee's right to organize under the National Labor Relations Act, may not retaliate against a whistleblower or because the employee asserts his or her employment-related rights (for example, asking to be paid overtime) and may not discriminate against an employee because of his or her race, religion, age or other protected status. Anytime an online posting may implicate these potential risk factors, the employer must evaluate the risk before terminating or disciplining the employee. An online post that may strike the employer as disrespectful and grounds for discipline ("ABC Corp doesn't care enough about its employees to pay us fairly for our work"), is likely protected by law.

Whistleblowing

Many states, including Oregon have enacted whistleblowing laws that potentially protect a wide range of employee communications. ORS 659A.199(1) provides:

> It is an unlawful employment practice for an employer to discharge, demote, suspend or in any manner discriminate or retaliate against an employee with regard to promotion, compensation or other terms, conditions or privileges of employment for the reason that the employee has in good faith reported information that the employee believes is evidence of a violation of a state or federal law, rule or regulation.

Significantly, this law does not require that the employee follow any particular reporting process (for example, reporting to a governmental agency) in order for the report to be protected. Various other laws protect industry-specific whistleblowing; for example, the Sarbanes-Oxley Act contains protections for employees of publicly-traded companies who report corporate fraud or accounting abuses. An employer that desires to discipline or fire an employee for the employee's online expression should evaluate the posting to determine whether it may be considered a form of whistleblowing and therefore a protected activity.

Concerted Activity

In union and non-union workplaces alike, employee communications about pay, benefits and working conditions may be protected as concerted activity under the National Labor Relations Act ("NLRA").[10] The NLRA protects "concerted activities" for the "mutual aid and protection" of employees. One commentator has noted that "* * * employee websites with the overt goals of encouraging concerted employee action, encouraging dialogue regarding employment issues, or that generally speak for other similarly situated employees have been protected by section 7, as have other analogous electronic media forms."[11]

---

[10] 29 USC § 157.

[11] Andrew F. Hettinga, Student Note: Expanding NLRA Protection of Employee Organizational Blogs: Nondiscriminatory Access and the Forum-Based Disloyalty Exception, 82 Chi.-Kent L. Rev. 997 (2007).

Before taking adverse action against an employee for posts, the company should ensure that the employee's actions are not concerted activities protected by the NLRA. Generally, posts that involve or touch upon the following topics should be analyzed for NLRA application before using such posts as the basis for disciplinary action:

- Wages, Salaries, or Hours
- Working Conditions
- Dress Codes
- Work Assignments
- Employment Policies or Actions
- Any Organizational or Union Advocacy

In November 2010, the NLRB filed a charge against American Medical Response (AMR) alleging that the ambulance service illegally terminated an employee who posted negative remarks about her supervisor on her personal Facebook page.[12] The complaint also alleged that the company illegally denied union representation to the employee during an investigatory interview, and maintained and enforced an overly broad blogging and internet posting policy.[13] The case was settled when AMR agreed to revise its policy prohibiting employees from making disparaging statements and to allow union representation in appropriate circumstances. Although the NLRB took the position that the AMR policy prohibiting disparagement of the employer was overly broad, in a December 2009 Advice Memorandum[14] the NLRB took the position that a similar policy was not overly broad.[15] It is probably safe to say that the NLRB's view of employer social media policies is evolving.

---

[12] http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments

[13] AMR's policy reportedly prohibited employees from "making disparaging, discriminatory, or defamatory comments when discussing the Company or the employees' supervisors, co-workers and/or competitors."

[14] *Sears Holdings (Roebucks)* , NLRB Case No. 18-CA-19081.

[15] http://www.employerlawreport.com/uploads/file/Advice%20memorandum.pdf . The policy included the following: "[I]n order to ensure that the Company and its associates adhere to their ethical and legal obligations, associates are required to comply with the Company's Social Media Policy. The intent of this Policy is not to restrict the flow of useful and appropriate information, but to minimize the risk to the Company and its associates. In order to maintain the Company's reputation and legal standing, the following subjects may not be discussed by associates in any form of social media:

• Company confidential or proprietary information
• Confidential or proprietary information of clients, partners, vendors, and suppliers
• Embargoed information such as launch dates, release dates, and pending reorganizations
• Company intellectual property such as drawings, designs, software, ideas and innovation
• Disparagement of company's or competitors' products, services, executive leadership, employees, strategy, and business prospects
• Explicit sexual references
• Reference to illegal drugs
• Obscenity or profanity

There are limits to the protections offered employees for concerted activity. Speech that is disloyal, reckless or maliciously untrue may lose the protection of the NLRA. Certain categories of speech have been found to be unprotected, depending upon the circumstances, among them: (1) remarks that disparage the employer or its products; (2) confidentiality breaches; and (3) recklessly or maliciously false accusations.[16]

Inappropriately Accessing Social Media

Employers should be cautious regarding how they access employee web sites that require a password or access code. In *Konop v. Hawaiian Airlines, Inc.*,[17] an airline pilot, Konop, maintained a secure website where he posted information critical of his employer. Visitors to the website were required to log in with a user name and password. The terms and conditions of the website prohibited any member of Hawaiian Airline's management from viewing the website. A Hawaiian Airlines officer asked another pilot to register for a login and password and give the information to the officer. The pilot did so, and the officer viewed the website multiple times using the improperly obtained login information, became upset about the contents, and threatened to sue Konop. Instead, Konop sued his employer alleging that Hawaiian Airlines violated a range of laws. The Ninth Circuit Court of Appeals reversed the district court's grant of summary judgment in favor of Hawaiian Airlines, allowing Konop to proceed with his claims that Hawaiian Airlines violated the Railway Labor Act (an Act analogous to the NLRA) and violated the Stored Communications Act.[18]

In another case, *Pietrylo v. Hillstone Restaurant Group*,[19] the court held that the employer violated the federal Stored Communications Act and the New Jersey Wiretapping and Electronic Surveillance Control Act by secretly monitoring employees' postings on a private password-protected Internet chat room. In *Pure Power Boot Camp, Inc., et. al., v. Warrior Fitness Boot Camp LLC et al*, Case No. 1:08-cv-04810-JGK-THK (D. NY 2010), the court determined that an employer who was able to view its former employee's Hotmail account after the former employee's password automatically populated the sign on field was liable for violating the federal Stored Communications Act.[20]

Public employees have greater privacy rights, arising from the Fourth Amendment. Nonetheless, in a recent decision, the Supreme Court held that a police agency did not violate its employees' rights by viewing police officers' text messages to determine whether officers were spending an inordinate amount of work time engaging in personal text conversations.[21] The decision was based in part on the City's policy, which stated: "[The City] reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." Even assuming the officers had an expectation of privacy in the texts, the Court concluded that

---

• Disparagement of any race, religion, gender, sexual orientation, disability or national origin."

16 *When Is Employee Blogging Protected by Section 7 of the NLRA?*, Katherine M. Scott, 2006 Duke L. & Tech. Rev. 0017. http://www.law.duke.edu/journals/dltr/articles/2006DLTR0017.html.

17 302 F3d 868 (9th Cir 2002).

18 18 USC §§ 2701-2710.

19 2008 WL 6085437 (DNJ 2008).

20 http://www.tradesecretslaw.com/uploads/file/order2.pdf

21 City of Ontario, California v. Quon, 130 S. Ct. 2619 (2010).

because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable and the Fourth Amendment had not been violated.

Policies spelling out the employer's right to monitor an employees' internet activities during working time can be helpful in defeating an employee's claim that the employer invaded the employee's privacy by reviewing computer records to determine the internet sites visited by the employee from his work computer. [22]

C. Who Owns the Blog, Fan Page, or Twitter Account?

It is not uncommon for a sales employee to set up a fan page for a product and to build a substantial following. This can be a problem if the employee goes to work for a competitor, taking his "fans" with him and requiring the company to start over from square one in its social media marketing efforts.[23] In the United Kingdom, an employer went to court to force a former employee to turn over information on his business contacts built up through use of business contacts built up through use of LinkedIn.com.[24] Having a policy and/or a signed agreement in place may save a lot of headaches for employees charged with social media responsibilities on the employer's behalf.[25] If you are paying for a blog or an account, and/or for the employee to spend time blogging on the company's behalf, then such a policy or agreement should definitely be in place to protect the company's rights. In the absence of such materials, your company may be in the uncomfortable position of being the first test case of the "default" rule in your jurisdiction.

Companies generally want to make sure their social media accounts are clearly company-branded, company paid-for and otherwise have clear indicia that they are not personal accounts. Conversely, the company generally cautions employees who post about work to disclaim that the employee speaks on behalf of the company.

D. When Is Your Company Responsible for Employee Statements on a Personal Website?

It is difficult with social media to entirely separate the business from the personal. Even on a personal Facebook account, a large percentage of people list their employer, their profession or their work e-mail address, which ties that account, to some extent, back to the company. Further, some employers actively encourage their employees to blog to increase the company's

---

22 *Thygeson v. US Bancorp*, 2004 U.S. Dist. Lexis 18863 (D. Or. , Sept. 15, 2004).

23 *See generally, Who Owns What in Social Media?*, http://humanracehorses.blogspot.com/2009/05/who-owns-what-in-social-media.html (May 29, 2009); *Who Owns Your Twitter or Facebook Connections?*, http://www.theharteofmarketing.com/2009/03/who-owns-your-twitter-or-facebook-connections.html.

24 *See* Brian Van Wyk, *Note: We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vanderbilt J. of Ent. And Tech. Law 743 (2009), available at http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3982 (discussing the lawsuit brought by Hays Recruitment against its former employee Mark Ions).

25 *See generally, Do You Have a Social Media Non-Compete?*, http://www.ducttapemarketing.com/blog/2009/04003/do-you-have-a-social-media-non-compete/.

profile. It is therefore problematic to assume that employees' use of social media will not be imputed to the company under certain circumstances.

One way in which to reduce an organization's liability exposure is to utilize an appropriate social media policy that requires a disclaimer by the employee that they are blogging or Twittering or Facebooking for themselves and not on behalf on the company. Another important requirement is that the employee appropriately and truthfully disclose their identity. If there are specific regulatory requirements that apply to your profession (financial services, health care industry), then employees should also understand how their behavior online may conflict with any applicable confidentiality requirements.

Another method of self-help is affirmative monitoring of social media for potentially problematic situations. However, there are pros and cons to monitoring social medial. For example, a company may decide to monitor mentions of their company name in social media, or make use of a third-party service[26] to do so on its behalf. This is likely to help nip problems in the bud, before clients, customers, or employees become aware of the issue. Monitoring, however, may also increase the risk of liability if the company fails to take appropriate action after discovering some types of activity. For example, in *Doe v. XYC Corp.*,[27] the employer discovered that an employee was visiting pornographic websites while at work. The company took ineffective action. Subsequently, it was discovered that the employee was taking inappropriate pictures of his 10-year-old stepdaughter and using his office computer to publish the photos on the Internet. The child's mother instituted a lawsuit against the company, and a court agreed that the employer, under the circumstances, was under a duty to investigate further and take effective action. In other words, if you decide to monitor, you should be prepared to do something about what is discovered.

E. FTC Regulation

The FTC has recently updated its guidance on truth-in-advertising to make it clear that an employee may not promote their employer's products or services on their blog, Facebook page, Twitter or other Internet media without disclosing the employee's relationship to the company. "When there exists a connection between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement (*i.e.*, the connection is not reasonably expected by the audience), such connection must be fully disclosed."[28] An endorsement is defined as "* * * any advertising message (including verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization) that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the

---

[26] *See, e.g.*, http://www.lanepr.com/lane-news/lane-pr-launches-social-media-services-for-online-reputation-management-employee-policies-and-communication-program-part-of-package ("LANE PR [Portland, Oregon] has developed a new online reputation management service. The service includes online reputation monitoring, online spokesperson training, tools and employee guidelines. The service is designed to help companies and their employees better build and manage their reputations online.")

[27] 887 A2d 156 (NJ Super 2005).

[28] 16 CFR § 255.5.

sponsoring advertiser * * *."[29] The following two examples deal with social media:[30]

> Q: My Facebook page identifies the company I work for. Should I include an additional disclosure when I talk about how great our products are?
>
> A: It's a good idea. People reading that discussion on your Facebook page might not know who you work for and what products the company makes. And many businesses are so diversified that readers might not realize the products you're talking about are sold by your company.
>
> * * *
>
> Q: A famous athlete has thousands of followers on Twitter and is well-known as a spokesperson for a particular product. Does he have to disclose that he's being paid every time he tweets about the product?
>
> A: It depends on whether his readers understand he's being paid to endorse that product. If they know he's a paid endorser, no disclosure is needed. But if a significant number of his readers don't know that, a disclosure would be needed. Determining whether followers are aware of a relationship could be tricky in many cases, so a disclosure is recommended.[31]

Many organizations' social media policies now address their employees' use of social media to promote the organization's products and services. Such policies may state, for example, that employees must state their relationship to the employer, that all statements must be truthful and not misleading, that employees must not disclose confidential company information on-line, that only designated employees may speak on behalf of the company and, if the employee is not one of the designated spokespersons, they must include a disclaimer on personal postings stating that the views expressed are their own and not those of the employer.

F. Examining a Range of Policies[32]

While social media policies are in the news, relatively few companies have actually implemented them. A 2009 survey[33] showed that only 17 percent of employers had plans in

---

29 16 CFR § 255.0(b).

30 http://www.ftc.gov/bcp/edu/pubs/business/adv/bus71.shtm.

31 16 CFR § 255.5.

32 A wide range of publicly-available policies are located at the Social Media Guidance website, http://socialmediagovernance.com/policies.php. This article also contains links to many different social media policies: http://www.searchenginejournal.com/why-employees-need-social-media-guidelines/12588/.

33 Aliah D. Wright, Employers, *Employees Shun Policies on Social Networking, HR Magazine* (SHRM Feb. 2010) (discussing Deloitte LLP's 2009 *Ethics & Workplace Survey* results).

place to examine and minimize potential risks to reputation related to use of social media. At the same time, almost half of employees surveyed stated that they regularly visit one or more social media sites four or more times per week. Over 53% of employees stated that "social networking pages are none of an employer's business." A social media policy (and/or related training) can help educate employees on why it sometimes is the employer's business what an employee is doing or saying online. The following policies are not provided as model or suggested policies but rather, simply to show a range of different approaches.

The Less Is More Policy[34]

There are two major benefits to adopting a very simple social media policy: (1) the policies are easier to remember and therefore perhaps more likely to make an impact on actual behavior; and (2) for industries and environments where employees exercise a fair amount of independence and discretion, employees are less likely to find the policy unduly restrictive or unreasonable.

Example: Zappos

Just Be Smart! (This is supplemented by more extensive employee training.)[35]

Example: The Australian Broadcasting Corp[36]

a. Do not mix the professional and the personal in ways likely to bring the ABC into disrepute.

b. Do not undermine your effectiveness at work.

c. Do not imply ABC endorsement of your personal views.

d. Do not disclose confidential information obtained through work.

A Somewhat More Detailed Policy

Example: WebTrends

In the spirit of best practices and partially inspired by Charlene Li/Forrester[37] *and Channel 9—our blogging code of ethics:*

---

[34] The Australian Broadcasting Corp.'s Social Media Guidelines are discussed at http://mindymcadams.com/tojou/2009/journalists-use-of-social-media/ and http://kevin.lexblog.com/2009/12/articles/social-media-1/a-simple-social-media-policy-for-law-firms/.

[35] http://www.clickz.com/3639435?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+clickzblog+(ClickZ+News+Blog).

[36] http://blog.clickz.com/090813-200136.html;http://www.searchenginejoumal.com/why-employees-need-social-media-guidelines/12588/ (in comments).

We will tell the truth. The whole truth and nothing but the truth.

We only delete comments that are spam, profanity, hate or infringe on copyrights. Offenders may be banned from commenting.

We will speak with our own voices, not glossy corporate speech.

We will correct any errors or omissions promptly, noting when we do.

If we disagree with other opinions, we will do so respectfully.

We will reply to comments, where appropriate, as promptly as possible.

We will link to references and source materials directly.

Please also consider the following when engaging with other people online:

Try to add value. Provide worthwhile information and perspective. WebTrends is best represented by its people and what you publish may reflect on all of us.

Respect your audience. The right time to jump into a conversation is when your contribution either solves a problem or relieves pain.

You are personally responsible for the content you publish on any form of user-generated media. Be mindful that what you publish will be public for a long time—protect your privacy, as well as ours. Respect copyright, fair use and financial disclosure laws.

Identify yourself and your role at WebTrends when you discuss the WebTrends or WebTrends-related matters. Make it clear that the views expressed are yours and do not necessarily represent the views of your employer. Know and follow our general business conduct guidelines.

Example: Software Company

The Company community has opened an area in which users can maintain a blog (among other services). The Company encourages employees to participate in this same community—whether you are obsessively writing about the browser, or about nothing but your favorite Norwegian (or sub-Saharan) wildflowers.

Sometimes Company employees may want to write about something but worry that it is not for disclosure. This may lead to a missed opportunity to talk about something that is, in fact, public. They also may not realize that something is strategically sensitive and should not be written about.

---

[37] *See generally*, http://blogs.forrester.com/groundswell/2004/11/blogging_policy.html.

To shed some light on these issues, Company employees may refer to the following guidelines:

Share your thoughts

Be open and use this service for discussing life at the Company, or talking about topics outside of work. This area is yours, use your personality and use your language, whether that's English, Norsk, casual, refined, techy-jargon, or Pig-Latin.

Be active

Interact with other community members, both inside and outside the Company. We want to encourage other users to become active in the community too.

We're not your mama

No one is here to look over your shoulder, but please use common sense when it comes to the use of objectionable language, sensitive topics, etc. Also be sure to proof-read and use proper grammar/spelling.

Don't give away the farm

Remember your obligations to your NDA. If an item is questionable, in terms of secrecy (unreleased versions, release dates, project names, features under development, status of internal development, etc), it may be better to err on the side of caution as we are under strict obligations of secrecy with our partners. If you have specific questions, feel free to bring them up with your manager.

Check your sources

Some sources may acquire inside knowledge that is not meant for publication. Just because you may see something on the Web does not mean it is meant to be public knowledge. As a general rule, an item that has appeared in a press release may be considered fair game.

Our friends are your friends

Remember to protect the privacy of the Company's partners and customers. If there's a new deal with Widget Co. that has not been mentioned in a press release, it is probably not public knowledge.

For the squeamish

Some may feel more comfortable posting a disclaimer claiming that the opinions posted are not those of the Company. This may help readers understand that your comments are from your perspective.

Above all

Remember to use common sense. If you need help in a situation, don't hesitate to ask your manager. Your blog is meant to be an open window, but remember there are legal obligations.

A More Restrictive Policy

Some companies discourage the use of social media for a variety of reasons. One common concern is that employees will be less productive if they have access to social media at work. Another reason for restricting social media use is simply an attempt to reduce the company's exposure to associated liability risks. Obviously, these types of restrictive policies will be more appropriate in some industries and work environments than in others. The California Chamber of Commerce (HR California)[38] offers this restrictive policy language:

> *The Company does not use or does it condone the use of social media in the workplace for any purpose. Social media is a set of Internet tools that aid in the facilitation of interaction between people online. Use of Internet based programs such as Facebook, Linked In, and Twitter (this is not meant to be an exhaustive list—if you have specific questions about which programs the Company deems to be social media, consult with your supervisor or HR) is a violation of Company policy and use of these programs either on Company-owned property or on your personal property during work hours on the work premises can result in discipline up to and including termination.*

The Comprehensive Policy

A search on the Internet for social media policies leads to many references to Intel's policy.[39] As a large technology company with its own blog and many tech-savvy employees, presumably Intel has had to think through many of these issues a bit earlier and more thoroughly than other organizations.

---

38 http://www.calbizcentral.com.

39 *See* http://www.intel.com/sites/sitewide/en_us/social-media.htm.