Cybervetting refers to the practice of viewing social networking sites such as MySpace and Facebook, blogs and microblogs like Twitter and using search engines like Google and Yahoo! to obtain information about job applicants or to monitor current employees. In a 2009 Careerbuilder.com survey conducted by Harris Interactive, 45 percent of employers reported having used social networking sites for such purposes, a significant jump from 22 percent the previous year. The survey reported that another 11 percent planned to do so. Thirty-five percent of employers surveyed indicated that they found information that caused them not to hire the candidate. Fifty-three percent found provocative or inappropriate photographs or information; 44 percent found content about candidates drinking or doing drugs; and 35 percent discovered bad-mouthing of a previous employer, co-workers or clients.

A more recent survey conducted by Microsoft indicated that 79 percent of U.S. human resource professional respondents used online information to evaluate candidates most or all of the time and that this type of evaluation is part of their formal hiring process. A whopping 84 percent of those surveyed believed it is appropriate to consider a candidate’s online reputation when evaluating that person for a job. Seventy percent have rejected a candidate based on information obtained online about a candidate.

In addition to using social networking sites to vet potential employees, employers are increasingly monitoring their current employees’ online activities (including social networking sites) even in the absence of a specific policy. The Society of Corporate Compliance and Ethics and the Health Care Compliance Association conducted a survey in 2009, polling 800 individuals at for-profit, nonprofit and government institutions. Fifty percent of those respondents did not have a specific policy in place addressing employee use of social networking sites. If respondents did have a policy, 34 percent included it in a general policy on online usage while only 10 percent specifically addressed the use of social networking sites. Fifty-three percent reported that their organizations either do not monitor such use, haven’t had an issue or have a "passive" system in place (acting when an issue arises). Despite respondents indicating few policies in place, 24 percent of respondents reported having to discipline an employee for social networking activities.

Legitimate reasons to cybervet abound, from confirming a candidate's qualifications, scrutinizing writing or communication skills, and ensuring that a candidate is a good fit to preventing negligent hiring claims. For those already hired, an employer might check out a MySpace or Facebook page to confirm an employee's claim of disability or illness; to substantiate that a person is passing trade secrets or classified, proprietary or sensitive information; or to corroborate suspected criminal or other illegal activity. An employer might monitor online activities to scrutinize employee productivity or to prevent misuse of such technology.

Legitimate reasons aside, the practice of monitoring employees' workplace computers or cybervetting job candidates carries some legal risks. Public sector employers must be mindful of the relevant legal issues before embarking on this activity.

**Discrimination**

Hiring decisions or adverse employment actions must be based on unbiased legal considerations. Decisions based on race, color, gender, disability, age and national origin are prohibited under various federal and state laws, but information relating to these factors may be inadvertently discovered during cybervetting.
Take, for example, the employer who has a female employee who competently does her job. When the employer visits her Facebook page, he is surprised to learn that the employee is three months pregnant and demotes her to a position of lesser responsibility. Because the candidate is a member of a protected class and Title VII prohibits sex discrimination, which specifically includes pregnancy-based discrimination, the employer's knowledge of her status may form the basis of an employment discrimination claim. The employer will have to show that a legitimate, job-related consideration was the basis of its employment decision to counter such claims.

National Labor Relations Act Violations
The National Labor Relations Act (NLRA) defines five unfair labor practices for which an employer can be held liable. Section 8(a)(3) of the act prohibits discrimination in regard to the hiring, tenure of employment, or any term or condition of employment for the purpose of encouraging or discouraging membership in any labor organization. Claims of violations of the NLRA could be complicated with the addition of cybermonitoring. For instance, if employee union activity is discovered online by the employer, who then subjects the employee to an adverse employment action, the employee could potentially claim a violation of both the NLRA and invasion of privacy.

In Konop v. Hawaiian Airlines, a pilot maintained a personal and restricted website critical of his employer and labor concessions that the employer sought from the pilot's union. The employer accessed the website using another employee's login information and subsequently placed the pilot on medical suspension, which the appellant claimed was in retaliation for his union activity. The court held that the development and maintenance of the website was considered protected activity.

Invasion of Privacy
Some states may recognize the common law tort of invasion of privacy if an employer accesses an employee's social networking site and an employer makes an adverse employment decision based on the applicant's lawful off-duty activities.

In Pietrylo v. Hillstone Restaurant Group, an employee created a group on MySpace for employees of a Houston's restaurant to vent about work issues "without outside eyes spying on us." The site was by invitation only and was password-protected. One of the invited employees was asked by management for access to the site, and she complied, fearing an adverse employment action. The MySpace site included sexual remarks about managers and customers, references to violence and illegal drug use, jokes about specifications for customer service and quality, and more. Pietrylo and another employee were subsequently fired after management viewed the site.

Pietrylo claimed that management violated New Jersey's common law right to privacy. A jury subsequently found in favor of the restaurant on the right to privacy claim, stating that the plaintiff had no reasonable expectation of privacy with the site. However, the jury also found that the intimidating manner in which the defendant accessed the site violated the Stored Communications Act, 18 U.S.C. §§ 2701–11, and a similar state statute, both of which protect the privacy of web-based communications. The jury awarded the plaintiffs $3,400 in compensatory damages and $13,600 in punitive damages.

In June, the Supreme Court decided Ontario v. Quon, a case which interested privacy experts. Unfortunately for those who eagerly anticipated the decision, the Court sidestepped the issue of whether Quon, a public employee and SWAT team member, had a reasonable expectation of privacy in text messages transmitted on a government-issued pager. The Court noted that because of rapid changes in emerging technology that could have far reaching implications, the case would be decided on narrower grounds. Whether or not Quon had a reasonable expectation of privacy, the Court held that the search was justified because there were reasonable grounds for suspecting the search was necessary for a noninvestigatory work-related purpose and the search was not excessively intrusive. The Court noted that contrary to the Ninth Circuit's opinion, the city was not required to use the least intrusive means possible. (See sidebar for more discussion on Quon.)

First Amendment
It's not hard to imagine an employer disciplining or firing an employee for disparaging online posts about manage-
ment. And in our current litigious environment, it's not hard to imagine an employee claiming a violation of the First Amendment. For public employees, this argument is usually unsuccessful.

In Curran v. Cousins, a corrections officer was fired by the sheriff's department for posting messages on the union's public discussion web board comparing department administrators to Nazis and urging insubordination. The court noted that a government entity has broader discretion to restrict speech when it acts as an employer, but the restrictions must be directed at speech that has some potential to affect operations. In this instance, the court held that the posting was of public concern because Curran accused a public official of basing personnel actions on political affiliation rather than merit. The department also had adequate justification for firing Curran because his postings urged insubordination and were insulting and defamatory; in essence they were disruptive and threatening to government operations. Because the department is a law enforcement agency, the court held that there was a heightened need for order and harmony and that this need outweighed Curran’s First Amendment interests.

A similar case is Richerson v. Beckon, where a school official was demoted from curriculum specialist to a classroom teacher after she posted messages to her blog criticizing her employer, union representatives and fellow teachers, causing several employees to refuse to work with her. The court held that her speech disrupted co-worker relations and therefore demonstrated actual injury to the school’s legitimate interests, outweighing Richerson’s First Amendment interests.

**Veracity of Information and Defamation/Libel**

Microsoft’s survey indicated that 90 percent of U.S. human resource professional respondents were either very or somewhat concerned about authenticity of information found online. Because of the difficulty in verifying online content, employers who make snap judgments about their employees without first confirming facts through alternative sources, do so at their peril.

Generally, under state law, employees or candidates can sue under theories of defamation or libel if they can prove that harm resulted from a false and defamatory statement made in an unprivileged communication to a third party and the fault of the defendant amounted to negligence if not malice or reckless disregard. In the case of public officials, courts have held that the statement must be made with actual malice. A defendant may assert truth as an absolute defense.

---

**Ontario v. Quon: Cautious Decision or Shirk of Responsibility?**

When the city of Ontario, California, issued text pagers to its SWAT team members, no formal policy governed their use; only a general computer usage policy existed that stated that the email system and access to the internet were not confidential and were subject to review at any time.

Lt. Stephen Duke told SWAT team members that they could pay for charges in excess of the department's 25,000-character limit and that their messages would not be viewed to determine which were personal and which were government-related.

Duke became weary of his role as bill collector; and after Sergeant Jeff Quon went over the allotted character limit several times, the city requested transcripts of his text messages from the wireless vendor. The transcripts revealed that many messages from Quon's pager were personal and often sexually explicit.

The appellants asserted that they had a reasonable expectation of privacy under the Fourth Amendment with respect to the text messages and that the search was unreasonable as a matter of law. The Ninth Circuit agreed, even while stating that "[w]e do not endorse a monolithic view of text message users’ reasonable expectation of privacy as this is necessarily a context-sensitive inquiry." The Ninth Circuit held that because Duke assured team members that he would not audit their pagers as long as they agreed to pay for the overages and because Quon had previously exceeded the character limit without anyone reviewing his messages, Quon had a reasonable expectation of privacy.

In failing to uphold the Ninth Circuit's decision, the Supreme Court decided stopped short of making any broad pronouncements on the Fourth Amendment providing privacy to government employees in their electronic communications. At least one blogger thinks the case hints that the justices are sensitive to such issues. In SCOTUSBLOG, reporter Lyle Denniston notes the Court made it quite clear that this is an issue the justices take seriously and are hesitant about getting it wrong while the technology and cultural habits are still developing.

However, Justice Scalia, in his concurrence criticized the majority for not applying the Fourth Amendment to new technologies, stating that even though it may be difficult, "but when it is necessary to decide a case, we have no choice." Scalia added that "[t]he-times-they-are-a-changin’ is a feeble excuse for disregard of duty."
While libel is difficult to prove and no case law yet exists where the employer relied on information obtained on the internet, one can envision a set of circumstances where a former employee or candidate would prevail.

Consider the situation where the employer finds false online information that leads the employer to believe that an employee is padding travel reimbursement reports. The employer fires that individual and later sends an email to other employees naming the fired employee and warning them to comply with the travel reimbursement policy. Since the employer republished information that was false, the employer could be liable for defamation.34

**Terms of Service (TOS) Violations**

Questions have arisen as to whether employers using social networking sites to cybervet potential employees or monitor current ones are violating terms of service agreements. In the Bozeman, Montana, situation, a Facebook spokesman acknowledged that disclosing passwords violates its terms of service, which states that "[y]ou will not share your password, let anyone else access your account, or do anything else that might jeopardize the security of your account."35 Additionally, a Facebook representative told ABCNews.com that the policy might also have violated applicants' personal privacy.36

**The Need for Well-Crafted Policies**

In Stengart v. Loving Care Agency,37 an employee sent emails to her lawyers using the employee's personal password-protected web-based email account but via her employer's computer. The employer accessed these messages, claiming that the employee waived her attorney client privilege. The employer relied upon its electronic communications policy stating that the company has to right to review, intercept, access and disclose all matters on the company's media systems with or without notice. The policy also stated that emails and internet use and communications are considered part of the company's business and should not be considered personal or private and that the principal purpose of electronic mail is for company business communications; however, it also states that occasional personal use is permitted.38 The court noted that the defendant had multiple versions of the policy and that the parties were in dispute regarding whether the policy was ever finalized or formally adopted.39 The court went on to discuss that the ambiguous wording of the policy purports to "reach into the employee's personal life without a sufficient nexus to the employer's legitimate interests."40 The court held that the appellant's communications were privileged.

Stengart surely serves as a cautionary tale about the importance of wellcrafted policies. Employers should create policies for both external use (when employers cybervet) and for internal use (when either employees or employers use social media sites).

**External use policies** should screen applicants in a uniform manner. These policies should

- list the social media sites that will be searched for each applicant;
- list the lawful information about applicants desired from every search;
- state that a neutral third party will conduct the search, screening all applicants using the lawful criteria outlined above; and
- prohibit any organization from "friending" an applicant to gain access to nonpublic social networking profiles.41

**Internal use policies** should

- indicate and acknowledge the employer's use for business purposes and the employer's intent to monitor employees;
- inform employees that misuse can be grounds for discipline, up to and including removal;
- indicate acceptable and unacceptable disclosure of confidential or proprietary information;
- prohibit false posting of information about the employer, its employees, or its clients;
- list someone within the organization as the point person for questions or issues about social media use; and
- instruct employees to use good judgment and take personal and professional responsibility for content.42

For more information and examples of current policies, see [www.socialmedigovernance.com](http://www.socialmedigovernance.com).
that employees "friend" them so that they have access? "The fundamental problem with this type of voluntary electronic befriending, however, is that an employer or supervisor may learn more information than they need or want about the employee or applicant," said William A. Herbert, deputy chair and counsel of the New York State Public Employment Relations Board and co-chair of the ABA Labor and Employment Section's Technology in the Practice & Workplace Committee. "Later, such knowledge may be cited in a legal claim alleging that an adverse employment action was motivated by that knowledge," he added.

Herbert, a frequent speaker and author on this topic, also notes that there could be future overtime claims under the Fair Labor Standards Act for time spent by an employee communicating with the employer through a social networking page.

Additionally, an employer might be subject to claims of negligent hiring if the employer fails to cybervet. If it is so easy to Google someone and discover, within seconds, information that demonstrates a legitimate reason that a person is unqualified for a position, won't employers be subject to claims of negligent hiring if the employer sees something troublesome but ignores it? Herbert points to the Microsoft study indicating that of those surveyed, three-quarters of U.S. companies mandate the cybervetting of applicants as a matter of policy. "Time will tell whether the increasing use of such vetting will be deemed by the courts to create a due diligence obligation for an employer to avoid liability in a potential future negligent hiring tort claim," said Herbert.

And what about neutral parties reviewing such information? Can human resources departments really be considered neutral, or is it worth the expense to hire an outside party to review? Philip M. Berkowitz, partner and chair of Nixon Peabody's international labor team, believes that most employers are likely to welcome the opportunity to outsource these responsibilities rather than relying on their own employees. "Employers will want to retain third parties who are capable of establishing best practices in this very fast-moving area," said Berkowitz. "These third parties will need to keep track of changes in social media sites and technology, as well as staying current with regard to government regulations. They will need to establish benchmarks for identifying appropriate sites to check, carry out appropriate training for individuals conducting the searches, and follow up as appropriate to verify and document the information learned." Berkowitz sees third-party review as a wise choice because there are simply too many variables for the average employer to control.

Final Words of Caution
Clearly, many unanswered questions and concerns about cybervetting and monitoring by employers remain. Technology is changing rapidly, and people are posting online an increasing amount of personal information about all aspects of their lives. In turn, employers are using this easily accessible resource to learn more about current or potential employees. Government employers must be vigilant to keep themselves informed of the type of cyberactivity that is appropriate and lawful. Model policies addressing these issues will be very helpful as employers travel through the minefield of cyberspace. (See sidebar about a project to draft such a model policy.)

Defense Personnel Security Research Center (PERSEREC) and the International Association of Chiefs of Police Team Up on Cybervetting Project

Even though cybervetting is pervasive, no generally accepted guidelines exist for employers. PERSEREC is working with the International Association of Chiefs of Police to change that.

The project has collected information about policies and practices pertaining to cybervetting and social media. Sources of information included news articles, scholarly works and written policies from various government, law enforcement, security and private-sector entities. This information was reviewed by subject matter experts (including human resource personnel, privacy advocates, tech experts, bloggers, industrial/organizational psychologists, lawyers, law enforcement personnel, government privacy officers, chief security officers and more) via an online survey.

Subject matter experts, stakeholders and affected practitioners will also share their thoughts and insights at focus group meetings to be held in 15 cities. The final goal is to develop cybervetting guidelines that achieve the right balance between individuals' constitutional rights and organizations' due diligence responsibilities.

The guidelines are expected to be available later in 2010.
Endnotes


2. Id.

3. Id.

4. Id.

5. Id.


7. Id.

8. Id.


10. Id.

11. Id.

12. Id.

13. Id.


18. 302 F. 3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003).

19. Id. at 884. But see Endicott Interconnect Techs., Inc. v. NLRB, 453 F.3d 532 (D.C. Cir. 2006) (An employee was dismissed after posting a message attacking management to a newspaper website’s public forum. The court held that his comments were so disloyal, disparaging and injurious that they were not protected by the NLRA.)


21. Id. at 1.


23. Ontario v. Quon, No. 08-1332, slip op. at 10-11 (June 17, 2010).


25. Ontario v. Quon, No. 08-1332, slip op. at 13 (June 17, 2010).

26. Id. at 15-16.

27. 509 F.3d 36 (1st Cir. 2007).

28. Id.

29. Id. at 47.

30. Id. at 50.

31. 337 F. App’x 637 (9th Cir. 2009) (unpublished/noncitable).

32. Id. at 638-639.

33. See supra note 8 and accompanying text.

34. See Noonan v. Staples, Inc., 556 F.3d 20 (1st Cir. 2009).


38. Id. at 394.

39. Id. at 395.

40. Id. at 399.

41. Philip M. Berkowitz & Jonathan M. Redgrave, Legal Challenges in Deploying Internal Corporate Social Media Tools, Webinar (May 6, 2010) (used with permission).

42. Id. =


44. Id. at n.9.