

Morgan Lewis

Web 2.0 in the Workplace


webcast

Eric Meckley

Ann Marie Painter

Christopher A. Parlo

Melinda S. Riechert



This communication is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2009 Morgan, Lewis & Bockius LLP. All Rights Reserved.

Technical Overview

- Webex Tech Support—866.779.3239
- Q&A tab is located on the bottom right hand side of your screen; choose “All Panelists” before clicking “Send”.
- Code for New York MCLE only, all other CLE credits will be processed automatically.
- Everyone will receive a copy of the presentation after the webcast.
- ONLY for attendees that are not able to hear audio through their computer speakers, you may join the teleconference. To do this, please:
 - Close the Audio Broadcast window.
 - Click on the REQUEST button on the Participants panel on the right-side of your screen to retrieve dial-in information.
 - Tech Support: If you are experiencing issues with your audio broadcasting, please call 866-779-3239.

Overview

Morgan Lewis

Web 2.0 Tools Used by Employees – Often During Work Hours

- Social Networking Sites (Facebook, MySpace)
- Business Networking Sites (LinkedIn, Plaxo)
- Online media (YouTube, Hulu)
- Twitter
- Personal Blogs
- Employer Sponsored Blogs





How Frequently Are Web 2.0 Tools Used?

- 22% of employees visit social networking sites 5 or more times per week; 23% visit social networking sites 1-4 times per week.
- 53% of employees say their social networking sites are none of their employer's business.
- 61% of employees say that even if employers are monitoring their social networking profiles or activities, they won't change what they're doing online – they know it's not private and have already made significant adjustments.
- 74% of employees say it's easy to damage a company's reputation on social media.

Source: http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics_workplace_survey_220509.pdf.

Recent Web 2.0 Usage Statistics

- Look at the increase in the use of Web 2.0 tools over a one-year period:

	April '08*	April '09	Change
	22.48	71.29	+ 217%
	58.75	54.60	- 7%
	1.22	17.10	+ 1298%
	47.26	50.37	+ 7%

*Visitors in Millions

Statistics from: Steven Johnson, Time, *How Twitter Will Change the Way We Live*, p. 36 (June 15, 2009) (citing Nielsen).

Employers Are Behind The Policy Curve

- 79% of employers frequently use social media to engage employees and foster productivity; 19% occasionally use social media; 1% rarely or never use social media.
- 45% of employers do not have a social media policy; 28% are working on developing one; 27% have a policy in place.

Source: The Buck Consultants/IABC “2009 Employee Engagement Survey” available at <http://www.iabc.com/rf/pdf/EmployeeEngagement.pdf>.

Newsworthy Risks...

- Whole Foods – CEO’s anonymous blogging promoting his company and criticizing competitors, including Wild Oaks Markets prior to hostile takeover, led to unfair competition claims/lawsuit following FTC/SEC investigation.
- Delta Airlines “Queen of the Sky” – Flight attendant fired for posting revealing photographs in company uniform on her blog. Sued for sex discrimination claiming men not similarly punished.
- Microsoft – Employee posted software upgrade prior to release on blog.
- Domino’s, Burger King, KFC – Employees posted video/photographs harming company image.

Key Legal Risks

- Hiring
- Trade secret or proprietary information disclosure
- Privacy
- Harassment
- Wrongful termination
- Defamation
- Disclosure of nonpublic material information creating securities law issues
- Negligent referral based on LinkedIn references
- Unauthorized use of company logos and copyrighted material

Key Opportunities

- Identifying a “lost witness” through Facebook or MySpace.
- Reviewing blogs, public Facebook postings, or Twitter comments for evidence undermining plaintiff’s liability theories and emotional distress allegations.
- A possible electronic discovery burden for employers ... and employees?

Key Legal Issues Involving Web 2.0 Issues In The Workplace

Morgan Lewis

Hiring Risks

- According to some reports, as many as 50% of employers and 77% of job recruiters concerned about alcohol/drug abuse, violence, and similar problems check out potential employees on the Web. *MySpace Is Public Space When It Comes to Job Search*, CollegeGrad.com, <http://www.collegegrad.com/press/myspace.shtml> (last visited July 27, 2008).
- In addition to the social networking sites, some employers also use search engines and other Internet sites such as PeopleFinders.com, Local.Live.com, Zillow.com, Feedster.com, Technorati.com (to search for blogs), and Opensecrets.org and Fundrace.org (to search for campaign donations). LaJean Humphries, *The Impact of Social Networking Tools and Guidelines to Use Them*, LLRX.COM, Jan. 15, 2007, <http://www.llrx.com/features/goodgoogle.htm>.
- According to the National Association of Colleges and Employers (the NACE), more than half of all employers use some kind of online screening technology including social networking sites like Facebook and MySpace. *Id.*
- Key issues: Lawful background checks? Invasion of privacy? Lawful off-duty conduct? EEOC background.

Defamation & the “Anonymous” Blogger

- When lawsuits are filed to discover the identity of an anonymous blogger, the courts balance the competing interests of the company and the blogger.
- *Krinsky v. Doe 6*, 2008 WL 315192 (Cal. App. 2008) (prima facie showing of defamation required before court would grant subpoena to Web host to obtain the identity of an anonymous blogger).
- But how often do anonymous bloggers register their real identities when securing an email address?

Defamation & the “Anonymous” Blogger

- Apple brought suit against unnamed individuals claiming they "had leaked specific, trade secret information about new Apple products to several online websites."
- Apple subpoenaed documents that would reveal the defendants' identities. The "John Does" brought a motion seeking a protective order based on their claim that they were "journalists" and thus entitled to invoke a privilege against disclosing their sources.
- Court ordered an ISP to identify people that Apple accused of stealing trade secrets and leaking information about Apple products through websites but left unresolved whether three ISP employees who claimed journalistic shield law protection of sources were indeed journalists.

Apple Computer v. Doe 1, et al., 139 Cal. App. 4th 1423 (2006).

Defamation Claims – By the Employer?

- Employer may sue former employees for defamation and invasion of privacy.
- “Cybersmearing” of employer by former employees. *Varian Medical Systems, Inc. v. Delfino*, Santa Clara County Super. Ct. No. CV780187 (Dec. 18, 2001): Santa Clara County, California jury awarded employer \$775,000 in compensatory and punitive damages against former employees for defamation and invasion of privacy).

Defamation Claims – By the Employer?

- Employer seeking injunctive relief must meet usual standard.
- *Bynorg v. SL Green Realty Corp.*, 2005 WL 3497821 (S.D.N.Y. 2005) (Court did not issue the employer an injunction to keep former employee from publishing false statements about it on her blog because of the strong presumption against prior restraints of speech and the established law against issuing preliminary injunctions in defamation cases, and because the employer failed to show irreparable harm.)

Defamation Summary

- An employer may be liable for defamatory statements made by an employee if the employee had the apparent authority from the company to speak on its behalf, under theories of ratification, respondent superior, or negligent supervision/retention.
- Therefore it is important that a company take steps to ensure that employees are not speaking on its behalf, and take prompt action against employees once it learns of any wrongful conduct.

Invasion of Privacy

- Invasion of privacy consists of four different theories: intrusion upon seclusion, publicizing private facts, false light, and appropriation of name or likeness.

Invasion of Privacy

- The town of Bozeman, Montana, required job applicants to provide passwords to email (Google, Yahoo!) and social networking (MySpace, Facebook) accounts.
- 98% of people believed this policy to be an invasion of privacy.
- On June 22, 2009, the town rescinded the controversial policy.

Invasion of Privacy

- Email: Several cases hold an employee does not have a reasonable expectation of privacy in email sent or received from the employer's computer or email system.
- *But see Brown-Criscuolo v. Wolfe*, 601 F. Supp. 2d 441, 449-50 (D. Conn. Mar. 9, 2009) (Court found that employee had a reasonable expectation of privacy in workplace emails after evaluating employer policy stating users have a limited privacy expectation despite routine monitoring and notice that personnel files may be discoverable under law.)

Privacy & The Stored Communications Act

- Federal Stored Communications Act (SCA): may prohibit employers from accessing and monitoring employees' online activities without proper authorization.
- Prevents employers from using illicit or coercive means to access employees' private social media accounts in an effort to root out critical or disgruntled employees.
- Can an employer retrieve keystrokes from an employee's work computer to access passwords and private social media account information?

Quon v. Arch Wireless Operating Co., 554 F.3d 769 (9th Cir. 2008).

- City police employee used a city-issued text message pager to send sexually explicit text messages.
- The text message provider, Arch Wireless, disclosed the text messages to the employer, the city police department.
- The Ninth Circuit ruled that this violated the SCA *even though the city was the subscriber on the service contract*.
- The court explained that the SCA prohibits providers of an “electronic communication service” — Internet Service Providers (ISPs) and text message services, for example — from disclosing stored e-mail or text messages without the consent of the sender or recipient.
- But, Ninth Circuit’s decision expressly reaffirmed the well established rule that employers can defeat an employee’s expectation of privacy by distributing a policy unambiguously stating that employees’ communications using corporate resources will be monitored and are not private.

Privacy & The Attorney-Client Privilege

- *Stengart v. Loving Care Agency, Inc.*, 2009 N.J. Super. LEXIS 143 (June 26, 2009)
- Emails were sent by an employee to her attorney using the company computer but from her personal email account. The emails were recovered by the employer from the temporary Internet files on the company computer but were originally sent through the employee's Web-based password protected email account. Were the emails privileged?
 - Lower court held emails were not privileged, relying upon the fact that the Employee Handbook warned: "Email and voice mail messages, Internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee."
 - Overturned on appeal. The appellate court found that the attorney-client privilege substantially outweighed the employer's argument that the emails were company property because they were sent from a company laptop.
 - Case remanded for a ruling disqualification or other sanctions against employer's counsel.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002)

- Pilot maintained website that only authorized employees could visit. Authorized employees voluntarily gave password to an unauthorized employee who accessed the site. Plaintiff sued his employer under the SCA for unauthorized access to his website.
 - Unauthorized access and review of the contents of a password protected web site can constitute violation of the SCA.
 - Employer's accessing without authorization of such a website can constitute impermissible surveillance of union-organizing activities in violation of the Railway Labor Act.
- Court held that employer violated the SCA because the authorized employees had never actually accessed the site and therefore were not authorized “users.”
 - The SCA "allows a person to authorize a third party's access to an electronic communication if the person is 1) a 'user' of the 'service' and 2) the communication is 'of or intended for that user.'"

Van Alstyne v. Elec. Scriptorium Ltd., 560 F.3d 199 (4th Cir. 2009)

- Company president gained access to employee's personal email account and admitted to accessing her account at all hours of the day for more than a year after her termination.
- Employee filed suit under the SCA, which the president attacked based on the employee's admission that the president's conduct had caused no actual damages.
- Although statutory damages under the SCA were not available to the employee, the U.S. Court of Appeals for the Fourth Circuit allowed punitive damages and attorneys' fees, even absent a showing of actual damages.

*Pietrylo v. Hillstone Rest. Group d/b/a
Houston's (D.N.J., No. 06-5754, jury verdict
6/16/09)*

- Two New Jersey waiters were fired after their managers took offense to comments they posted on a password protected MySpace account for restaurant staffers.
- A third employee gave managers her password to access the account, but claimed she was coerced into doing so.
- Jury found:
 - Managers had violated the SCA and the New Jersey Wire Tapping & Electronic Surveillance Act by intentionally accessing the MySpace page without authorization
 - The jury awarded \$17,003, including \$13,600 in punitive damages
- Defendant liable for plaintiffs' attorneys' fees.

Michigan Mayor Accidentally Posts Personal Employee Data on Twitter

- Mayor, intending to send a link on Twitter to the city's check register showing the city's expenses, instead sent a link to a report with employee information, including Social Security numbers and wage garnishments.
- Twitter removed the link and the city is providing the employees a free subscription to an identity theft service.

NY MCLE Credit Information

In order to receive NY MCLE credits for this webcast, please write down the following alphanumeric code:

9WCWP2209

You will be asked to provide this code to our MCLE credit administrator after the webcast.

Risks to the Employer: Discrimination, Harassment, and Retaliation

- Title VII, NLRA, other federal and state antidiscrimination laws
- Potential liability risks for employers:
 - the employer's sponsorship of the content/blog comments,
 - ratification by inaction, and
 - obligation to take action to prevent or eliminate inappropriate content once on notice.

Risks to the Employer: Discrimination, Harassment, and Retaliation

- Potential Employer Liability for Harassment Via Blog
 - Usual standards for workplace harassment apply.
 - Employer who knew or should have known of employee's use of blog to harass other employees could face liability.
 - *Blakey v. Continental Airlines, Inc.*, 164 N.J. 38, 751 A.2d 538 (2000) (Company has a duty to take effective measures to stop employee harassment of a co-worker when it knows or should know harassment is taking place in the workplace or work-related settings; NJ Supreme Court remanded case to determine whether "Crew Member Forum" electronic bulletin board was sufficiently connected with workplace to allow liability.)
 - Does an employer have a duty to monitor private communications (off-duty blogging) of employees?

Risks to the Employer: Discrimination, Harassment, and Retaliation

- Employer viewing applicant's personal information on blog/social networking site may trigger protections of antidiscrimination laws.
 - Sites may contain information regarding age, race, national origin, disabilities, sexual orientation, and other protected categories
 - Difficult for employer to prove it did not view and rely upon the personal information if there is a later lawsuit.
 - Even if not unlawful, employer may be making employment decisions based on inaccurate information.

Adverse Action Based on Blog May Violate State Lifestyle Discrimination Laws

- California prohibits discrimination against employees for lawful activities conducted outside of the workplace. Cal. Lab. Code 98.6, 96(k).
 - *Grinzi v. San Diego Hospice Corp.*, 120 Cal. App. 4th 72 (2004) (employee properly discharged because of her membership in a private investment group that the employer believed was an illegal pyramid scheme).
- Several other states have similar prohibitions (Colorado, North Dakota, Connecticut, New York).
- Thirty states and the District of Columbia protect smokers, or others who use other lawful consumable products, from termination based solely on such activities.
- Other examples: political activities, alcohol/drug usage.

Risks to the Employer: Wrongful Termination

- New media terminology: “Dooxed” means being terminated because of Web or blog postings.
- Whether private sector employers can defeat public policy termination claims by employees complaining about work depends upon the circumstances.
 - *Marsh v. Delta Airlines, Inc*, 952 F. Supp. 1459 (D. Colo. 1997) (employee properly terminated for writing letter to editor of paper critical of employer)
- Potential First Amendment free speech claims by public sector employees.

Risks to the Employer: Wrongful Termination

- Employee terminated for complaining in blog that manager spends most of the day on personal phone calls.
 - Not likely protected conduct.
- Employee terminated for complaining in blog that manager discriminates against female workers.
 - May trigger antidiscrimination/antiretaliation statutes.

Risks to the Employer: Wrongful Termination

- Employee terminated for complaining in blog that company has a practice of encouraging poor reviews to avoid payment of bonuses or pay increases.
 - May trigger the National Labor Relations Act (NLRA).
 - So far, no case law addressing whether statements made in personal blog constitute protected “concerted activity,” but employers should be aware of this potential risk.

Risks to the Employer: Wrongful Termination

- Employee terminated for complaining in blog that manager is filing false earning statements.
 - Could potentially trigger protection under Sarbanes Oxley Act (SOX) and/or state law whistle-blowing statutes.
 - *SOX requires an employee to report unlawful conduct to a supervisor, regulatory or law enforcement, or Congress.*
 - Not yet apparent whether publication in a blog satisfies the reporting requirement – will likely depend upon the individual factual circumstances.

Risks to the Employer: Harm to Company Image

- Employee reveals details in blog about personal life that harm company image.
- Domino's, Burger King, KFC are obvious examples.

Risks to the Employer: Copyright and Fair Use

- *L.A. Times v. Free Republic*, 2000 WL 565200 (C.D. Cal. 2000).
- Defendant “bulletin board” website allowed members to post news articles to which they added commentary. Members posted the entire text of articles, including those from plaintiff’s website.
- Court held that defendant’s verbatim copying and posting of news articles onto its website was an attempt to exploit the market for viewing plaintiff’s articles online and such action was not protected by the Fair Use doctrine.
- Potentially a concern with employer-sponsored blogs or Electronic Bulletin Board’s.

What Employers Can Do To Minimize Risk

Morgan Lewis

What Employers Can Do to Minimize Risk

- Review internet/email policy and social media/social networking policy.
- Implement a blogging/social networking policy.
 - Make sure that it is a policy that can be enforced.
 - Do not be too much of a “big brother.”
- Implement a policy on whether recruiters, HR and hiring managers can access social networking sites on job applicants (and if so, with what restrictions).
- Prohibit accessing of private password protected social networking sites without proper authorization.
- Consider whether to prohibit employees from providing references on sites like LinkedIn and other professional networking sites.

What Employers Can Do To Minimize Risk

- Do not prohibit employees from discussing terms and conditions of employment.
- Investigate complaints of harassment or discrimination.
- Provide guidelines on appropriate terms of use.
- Set Google alerts to keep up with who is talking about the company and what they are saying.
- Ensure security of employer sponsored blogs.
- Ensure appropriate employment decisions are made.

Internet/Email and Social Media Policy

- Inform employees they have no reasonable expectation of privacy in any technology by the company.
- State that employer may record or monitor activities at its discretion.
- Obtain signed acknowledgements.
- Detail activities in which employees may not partake.
- Prohibit any action that could be seen as harassing.
- Enforce the policy and punish violators.
- Post the policy.

Blogging/Social Networking Policy

- Define “blogging” and “social networking.”
- Prohibit the disclosure of trade secrets, and proprietary and confidential information.
- Time spent blogging or on social networking sites should not interfere with job duties.
- Address the use of company logos, IP.
- Whether/when permissible to discuss company’s competitors, clients, vendors.

Blogging/Social Networking Policy

- Employees blog at their own risk and are personally responsible for content.
- Require a disclaimer: “The views expressed in this blog are my personal views and they do not necessarily represent the views or opinions of my employer.”

Blogging/Social Networking Policy

- Determine whether access to major online networking websites will be blocked from work computers.
- Include contact information for the person to whom questions or concerns about a blog or blogging should be addressed.

Security

- Ensure security of employer sponsored blogs using up-to-date technology.

Make Appropriate Employment Decisions

- Ensure employment decisions are based only on appropriate criteria.
- Verify information obtained from the Internet before basing employment decisions on it.
- Do not ask third party to “friend” an applicant to investigate background (privacy, ethical issues).

Rights of the Employer

- To discipline or terminate employees for disloyalty.
- To discipline or terminate employees for insubordination, harassment, intimidation, or other violations of company policy.
- To discipline or terminate employees for revealing confidential or trade secret information.
- To protect its company image.

Rights of the Employee

- Right to engage in legal off-duty off-site conduct.
- Right to freedom of speech.
- Right to protest working conditions and report illegal conduct.

Questions

Melinda S. Riechert

Partner
Palo Alto
650.843.7530
mriechert@morganlewis.com



Christopher A. Parlo

Partner
New York
213.309.6062
cparlo@morganlewis.com



Ann Marie Painter

Partner
Dallas
214.466.4121
annmarie.painter@morganlewis.com



Eric Meckley

Of Counsel
San Francisco
415.442.1013
emeckley@morganlewis.com

