

Morgan Lewis

Evolving Employee Rights In the Age of Web 2.0

Webcast

Presenters:

Renée T. Lawson

Carla B. Oakley

Howard M. Radzely

Melinda S. Riechert

James P. Walsh, Jr.

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.

Overview

Company Challenges with Social Media

- Companies are challenged to clearly define the distinction between personal and professional use of social media
- How do companies articulate what may and may not be said through social media, particularly with respect to company business?
- When does a person's personal commentary adversely impact business goals and objectives or expose the company to liability?

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

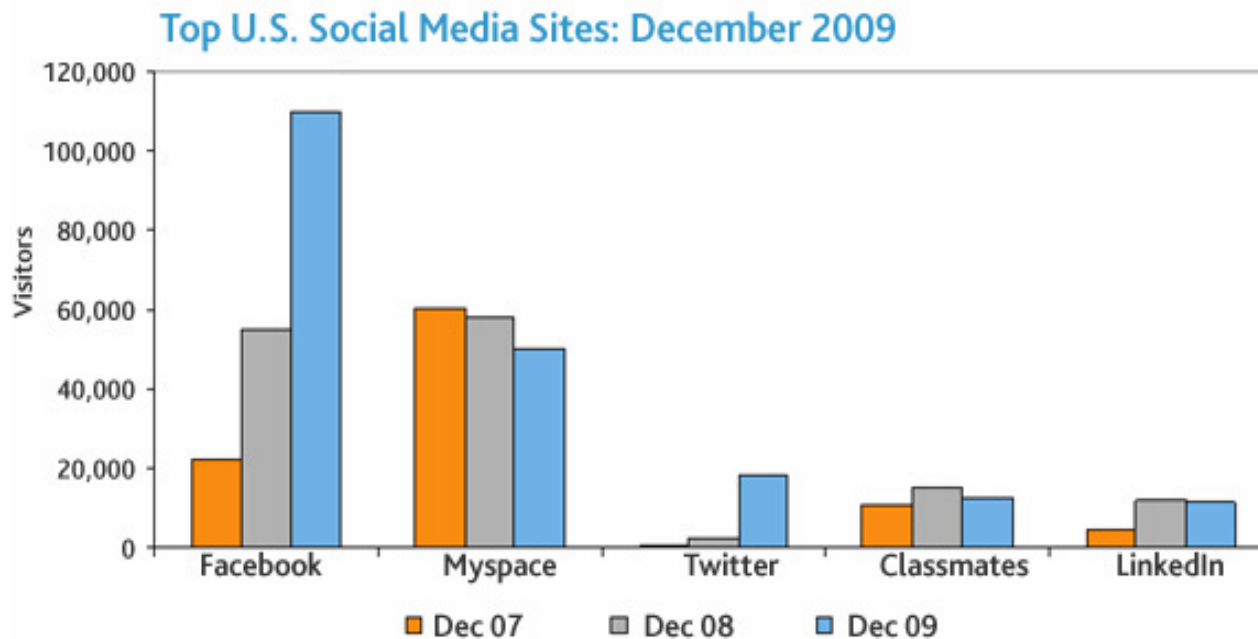
How Frequently Are Web 2.0 Tools Used?

- 22% of employees visit social networking sites 5 or more times per week; 23% visit social networking sites 1-4 times per week.
- 74% of employees say it's easy to damage a company's reputation on social media.
- 27% of employees say they do not consider ethical consequences of posting comments, photos, or videos online
- 72% of executives say their company does NOT have formal policies that dictate how employees can use social networking tools.

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

Web 2.0 Usage Statistics

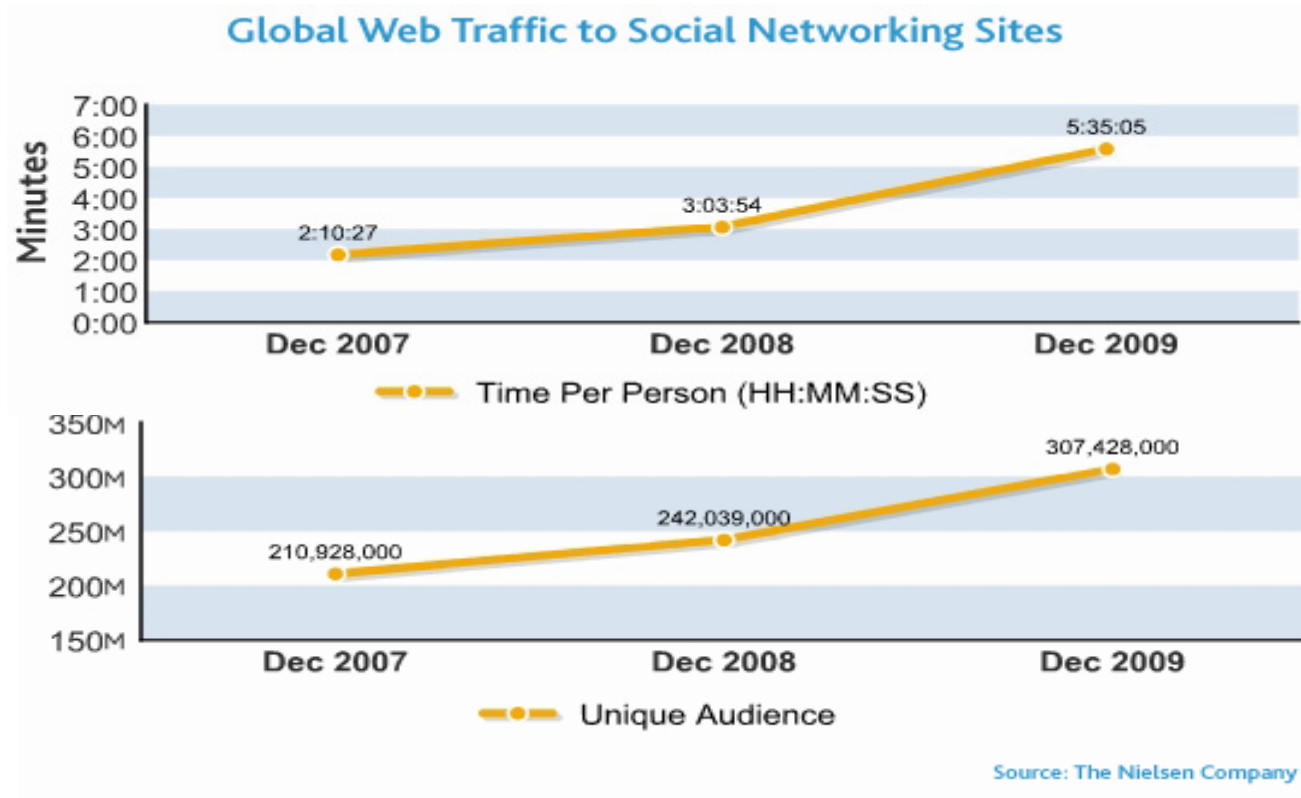
- According to The Nielsen Company, hours spent on social media sites have risen 82% in a one-year period.



Source: The Nielsen Company

Web 2.0 Usage Statistics (cont'd)

- Globally the time individuals spend on social media sites and the number of new individuals using these sites have grown steadily in the past two years.



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>.

What Control Does an Employer Have over Its Data
in the Cloud? – *The City of Ontario v. Quon* and
Electronic Communications Privacy Act

When Is Your Data Possibly Not Your Data to Control?

1. Reasonable expectation of privacy in data by someone else (e.g., employee)
2. Data controlled/stored by someone else (e.g., third-party vendor)

What Data Are All of Those Devices Creating, Accessing, and Storing in the Cloud?

- Substantial data other than email/calendar/contacts exists on mobile devices, e.g., text messages, “tweets,” music, photos, videos, Internet history, GPS, access to online storage solutions, etc.

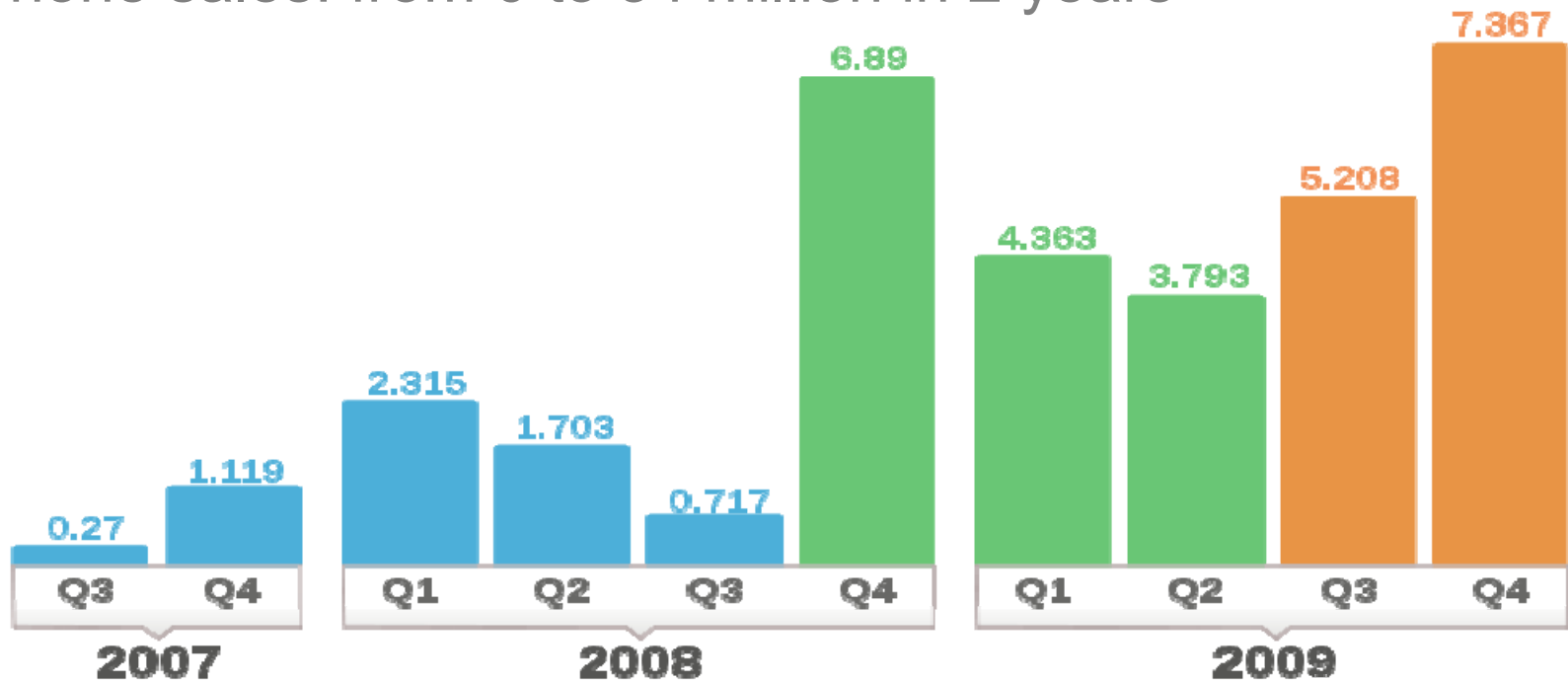


- “App” growth = exponential growth in data demand, volume, and type

Huge Growth in Mobile Devices and Usage

A new mobile device enters the consumer market every 3 days. (Source: Paraben)

iPhone sales: from 0 to 34 million in 2 years



iPhone sales per quarter Source: Wikipedia Commons

Privacy Issues

- Mobile device usage has become increasingly “personal”
- Companies frequently permit – even expressly in a policy – personal usage of company-issued devices
- Individual privacy laws are well established in some parts of the world (e.g., the European Data Protection Directive) and are building momentum in the U.S. (e.g., state laws, Electronic Communications Privacy Act (ECPA))

Administrative Control Issues

- The emergence of “cloud computing” enables third-party administration and control of basic technology services, including storage of data on remote noncompany devices
- Companies are outsourcing more and more of their data services, e.g., a third-party service provider manages company mobile devices

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

- City of Ontario (City) used a third-party service provider, Arch Wireless, to provide and manage its pagers
- City had an electronic use policy limiting communications to official use
- City allowed personal use of pagers if employees paid for such personal use
- City conducted audit regarding personal charges
- Arch Wireless disclosed to City text messages of police officers, including sexually explicit text messages of Sgt. Quon, resulting in a referral to internal affairs
- Sgt. Quon, his wife, his mistress, and another police officer sued the City and Arch Wireless for violation of the Fourth Amendment, California privacy rights, and the Stored Communications Act (part of the Electronic Communication Privacy Act)

Quon in the Lower Courts on Privacy and the Fourth Amendment

- Trial court: (1) reasonable expectation of privacy, but (2) reasonable search because audit focused on adequacy of character limit, not potential misconduct
- Ninth Circuit: (1) reasonable expectation of privacy, and (2) unreasonable search because less intrusive means existed to determine whether character limit was adequate
- Ninth Circuit 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.

Quon v. Arch Wireless (08-1332)

The Supreme Court Weighs in on Employee Privacy Interest in Company-Issued Mobile Devices

Justice Ginsburg:

- “If an employee is told, ‘now e-mails aren’t private, so we are warning you, we can monitor them,’ wouldn’t such an employee expect the same thing to apply to the pager?”

Chief Justice Roberts:

- “Now, most people will say, well, if you’re paying for them, they are yours. And it particularly covered messages off-duty. Now, can’t you sort of put all of those together and say it would be reasonable for him to assume that private messages were his business. They said he can do it. They said, ‘you have got to pay for it.’ He used it off-duty. They said they are not going to audit it.”

Quon in the Ninth Circuit on the ECPA

- The Ninth Circuit found a violation of the Stored Communications Act (SCA) even though the city was the subscriber on the service contract.
- Critical determination: Arch Wireless was an “electronic communication service” (ECS), not a “remote computing service” (RCS).
- Why does it matter what you call them? An ECS may divulge a stored communication only to the sender and a recipient, while an RCS is allowed to release it to the “subscriber.”
- HOLDING: An ECS – e.g., an Internet service provider (ISP) and text message service – may not disclose stored email or text messages without the consent of the sender or recipient, even if the requestor provides and pays for the service.
- NOTE: Supreme Court did not grant cert on this aspect of Quon.

Where Is the ECPA headed?

- Sen. Patrick Leahy, the Democratic chairman of the Judiciary Committee, said that "our federal electronic privacy laws are woefully outdated".
- The Digital Due Process Coalition seeks revisions of the ECPA to take cloud computing and privacy interests into account.
- House Judiciary Committee to hold hearings this spring on possible revisions.

What's at Stake?

A LOT

- Inability to get own data from third-party service provider
- Civil claims for privacy rights violations
- Statutory damages under the ECPA
- Criminal penalties under the ECPA

Lower Federal and State Courts on Workplace Privacy

Workplace Privacy & The Attorney-Client Privilege

Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54 (2009)

- Ms. Stengart exchanged emails with her attorney from her personal Yahoo!® email account using a company laptop. In anticipation of litigation, her employer recovered emails from the laptop's temporary Internet files, including those exchanged between Stengart and her attorney. Were the emails privileged?
 - Lower court held emails were not privileged because 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."
 - Appellate Division overturned that decision, finding 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.

Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010)

March 30, 2010 - New Jersey Supreme Court affirmed the Appellate Division

- Held that "under the circumstances" Stengart had a reasonable expectation of privacy in emails sent from her *personal* email account and that accessing a personal account from a company laptop did not waive the attorney-client privilege.
 - **Employer's Electronic Communications Policy was ambiguous:**
 - Policy stated that emails sent from employer's email system were "company property," *but* permitted "occasional personal use" of email system.
 - Policy was silent on personal, web-based email accounts, like Yahoo or Hotmail.
 - Policy did not warn employees that personal communications would be stored on the hard drive and could be forensically retrieved by the company, even after "deletion."
 - Stengart took reasonable steps to maintain the confidentiality of the emails by using a personal email account and protecting her password.
 - Emails contained boilerplate footer indicating that they may be privileged.

Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010) (cont'd)

- The court identified the following factors as relevant to whether the employee has an “expectation of privacy” in email communications:
 - Whether there is a clear company policy banning personal email use.
 - Whether the personal communications are sent via a company email account.
 - The location of the company’s computer (home office vs. employer’s place of business).
- The court specifically noted that its ruling “does not mean that employers cannot monitor or regulate the use of workplace computers.”
 - However, a policy that permits an employer to retrieve and read an employee’s *attorney-client communications* sent through a personal, password-protected email account (even if that personal account is accessed on a company laptop) is unenforceable.

Convertino v. U.S. Department of Justice, 674 F. Supp. 2d 97 (D.D.C. 2009)

- Convertino, a former Assistant U.S. Attorney, was charged with conspiracy to conceal evidence and lying to a Federal judge during a high-profile terrorism trial. He was acquitted, but confidential information regarding the investigation into his conduct was leaked to the media.
- Convertino sued the Department of Justice under the Privacy Act, 5 U.S.C. § 552a.
 - During discovery, the DOJ found emails between Assistant U.S. Attorney Jonathan Tukul (who was originally named by Convertino as an individual defendant) and Tukul's personal attorney. Tukul sent the emails using his DOJ email account and computer. He deleted the emails after sending them, but did not realize that archive copies remained on the server.
 - Tukul intervened in the lawsuit, asserting that the attorney-client privilege and attorney work product doctrine prevented disclosure of the emails.
 - Did Tukul waive ACP or AWP protection?

Convertino v. U.S. Department of Justice, 674 F. Supp. 2d 97 (D.D.C. 2009) (cont'd)

- Court analyzed the issue under Federal Rule of Evidence 502(b):
 - “A disclosure of a communication . . . covered by the attorney-client privilege or work product protection does not operate as a waiver . . . if the disclosure is inadvertent . . . and if the holder of the privilege or work product protection took reasonable precautions to prevent disclosure and took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error”
 - *“Mr. Tukul had no intention of allowing the DOJ, his employer, to read the e-mails he was sending to his personal attorney through his work e-mail account.”*
 - Tukul deleted the messages immediately, but did not realize a copy was kept on the DOJ’s server.
 - *Tukul intervened in the lawsuit to protect the privileged status of the emails.*

Convertino v. U.S. Department of Justice, 674 F. Supp. 2d 97 (D.D.C. 2009) (cont'd)

- “The question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.”
 - Whether the employer maintains a policy banning personal or other objectionable use;
 - Whether the employer monitors use of the employee’s computer or email;
 - Whether third parties have a right of access to computer or emails; and
 - Whether the employer notifies the employee—or the employee is otherwise aware—of the use and/or monitoring policies.
- Held: Tukul’s expectations were reasonable because the DOJ did not ban the personal use of its computer equipment and because Tukul was unaware that the DOJ was regularly accessing and saving emails from his workplace account.

What Employers Can Do to Minimize Risk

Internet/Email Policy

- Limit personal use of the company email system.
- Inform employees they have no reasonable expectation of privacy in any technology provided by the company (e.g., email, Internet, laptop, PDA).
 - All information forwarded or received via the company email system is subject to monitoring and may be stored.
 - All information sent, received or viewed on the Internet, including personal, web-based communications, instant messages, text messages or other forms of communication, can be stored on a computer's hard drive, the company's servers, etc. and can be reviewed and retrieved by the company at any time.
 - Back-up copies of electronic communications may exist, even if "deleted" from the computer.
- Issue periodic reminders to employees that the computers they are working on do not belong to them, and that information accessed on the computers may be subject to inspection and collection.

Internet/Email Policy (cont'd)

- Describe prohibited activities:
 - Disseminating confidential information;
 - Any actions that could be seen as harassing;
 - “Hacking” and related activities;
 - Tampering with or disabling security mechanisms on company computers;
 - Unauthorized downloads; and
 - Violations of copyright laws.
- Enforce the policy and punish violators.
- Obtain signed acknowledgements and post the policy.

Other Considerations

- Implement a policy on whether recruiters, HR, and hiring managers can access social networking sites re: job applicants (and if so, with what restrictions).
- Prohibit accessing private password-protected social networking sites without proper authorization.
- Do not ask a third party to “friend” an applicant to investigate background (privacy, ethical issues).

Other Considerations (cont'd)

- Consider whether to prohibit employees from providing references on sites like LinkedIn and other professional networking sites.
- Do not prohibit employees from discussing terms and conditions of employment.
- Investigate promptly complaints of harassment or discrimination.
- Set Google alerts to keep up with who is talking about the company and what they are saying.

FTC Rules

FTC Guides for Websites and Blogger Testimonials and Endorsements

- FTC Guides effective December 1, 2009
 - 16 C.F.R. Part 255
- Guides apply to testimonials and endorsements
 - Statements that consumers are likely to believe reflect the opinions, findings, or experiences of someone other than the advertiser
- Guides apply to statements by employees, as well as those by consumers, experts, organizations, and celebrities
 - Both advertisers and endorsers may be liable

FTC Guides for Websites and Blogger Testimonials and Endorsements (cont'd)

- Response to stealth marketing and undisclosed influences in marketing
- Guides provide the basis for “voluntary compliance with the law”
- FTC will use these guides to evaluate whether endorsements and testimonials violate FTC Section 5 (unfair practices statute)
- Consider private claims, e.g., unfair competition, unfair business practices, and false advertising

FTC Guides Require Disclosure of “Material Connections” Between Bloggers and the Companies They Promote

- Is blogger’s statement “sponsored”?
 - Is the blogger compensated by the company or a third-party marketer?
 - Was the product or service provided for free?
 - Is there any agreement between the blogger and the company?
 - What is the length of any relationship between the blogger and the company?
 - Has the blogger previously gotten products from the company, or does the blogger anticipate getting products in the future?
 - What is the value of the items or services received?
- Status as an employee is a material connection that must be disclosed.

Disclosure of “Material Connections” 16 C.F.R. § 255.5

- Connections that might “materially affect the weight or credibility of the endorsement”
- Must be “clearly and conspicuously” disclosed
- Disclosure need not be extensive or formal, but visible and clear
 - No formal FTC guidance on this issue yet

FTC Guide – § 255.5, Example 8

- Online message board discussing new music download technologies and products, with information exchanges about new products
- Employee of product manufacturer posting messages promoting the product
- Knowledge of the poster's employment would affect weight or credibility of comments
- Poster should clearly and conspicuously disclose relationship to readers

FTC Guides Encourage Development and Implementation of Policies

- Guides encourage companies to:
 - Monitor employees blogging on the company's behalf and other bloggers who are being paid or compensated in any way to promote its products
 - Take steps to halt continued publication of deceptive representations

FTC Guides Encourage Development and Implementation of Policies (cont'd)

- Guides create incentives for companies to create and implement policies, including:
 - Restricting employee and consultant endorsements on blogs, in tweets and on social media sites
 - Advising endorsers, including employees and consultants, of their responsibility to disclose material connections and truthfully describe the product or service
 - Advising blog advertising agency of approved product claims, and requiring agency to communicate such claims to bloggers

Employer Policies Reduce Risk

- FTC will consider whether a company has implemented appropriate procedures in deciding whether to bring enforcement actions
 - Actions of “rogue” employees violating company policy not likely to result in enforcement actions
 - FTC declined to specify procedures that should be implemented to confirm compliance with the Guides, acknowledging need for flexibility

Considerations for Policies for Employees and Consultants

- Require clear and visible disclosure of relationship to company when discussing company products or services
 - Consider requiring express disclaimer: “The views expressed in this blog are my personal views and do not necessarily represent the views or opinions of my employer.”
- Prohibit anonymous discussion of company products and services – promote transparency and protect confidentiality
- Prohibit employee/consultant from representing himself or herself as a spokesperson of the company
- Prohibit false, unsubstantiated, or misleading statements

Considerations for Policies for Employees and Consultants (cont'd)

- Remind employees that they blog at their own risk and are personally responsible for content
- Apply policy to all communications – blogs, tweets, social networking sites, wikis, etc.
 - Define “blogging” and “social networking”
- Disclose the company’s right to monitor postings, tweets, etc., and potential disciplinary actions
- Include reminders re: compliance with code of conduct, trademark and copyright policies, and confidentiality
- Identify a contact person who can address questions or concerns about a blog or Internet post

Key Risks for Employers

Hiring

- Should employers search the Internet or review the social networking sites of job applicants?
 - Several states have laws protecting legal off-duty off-site conduct (California, Colorado, North Dakota, Connecticut, New York).
 - Sites may contain information regarding age, race, national origin, disabilities, sexual orientation, and other protected categories
 - Is this a lawful background check?
 - *California law requires disclosure if decisions are made based on the information obtained.*

Hiring (cont'd)

- Is it an invasion of privacy?
- Even if lawful, employer may be making employment decisions based on inaccurate information.
- Should employers adopt a policy on whether, by whom and when its recruiters, HR professionals, and managers review publicly available information on job applicants?

Defamation

- 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.
 - The employer's sponsorship of the content/blog comments
 - Ratification by inaction
 - Obligation to take action to prevent or eliminate inappropriate content once on notice

Harassment

- Company may be held liable if it knew or should have known of harassment and failed to take appropriate action
 - *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.)

Wrongful Termination

- Can an employer be held liable for wrongfully terminating an employee based on the employee's social networking activities or information learned from the Internet?
 - Employees have right to complain about terms and conditions of employment
 - *Wages, benefits, working hours, the physical environment, dress codes, assignments, and responsibilities.*
 - *Must be concerted activity.*
 - Sarbanes Oxley Act and/or state law whistleblowing statutes.
 - Legal off-duty off-site conduct.
 - Megan's Law.
 - Employee's right of privacy.

Defamation of the Employer or Its Employees

- Recent case where company sued sender of defamatory tweet that went viral
- What can an employer do when an employee defames the company or its employees on a social networking site, tweet or blog?
- Seek an injunction:
 - *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 of the Employer or Its Employees (cont'd)

- Sue for damages:
 - *Varian Medical Systems, Inc. v. Delfino*, Santa Clara County (California jury awarded employer \$775,000 in compensatory and punitive damages against former employees for defamation and invasion of privacy.)

Defamation of the Employer or its Employees (cont'd)

- What if the employer does not know the identity of the blogger?
 - Filing John Doe lawsuits to discover the identify of the anonymous blogger.
 - *Krinsky v. Doe 6*, 2008 WL 315192 (Cal. Ct. App. 2008) (Prima facie showing of defamation required before court would grant subpoena to Web host to obtain the identity of an anonymous blogger.)
 - Unlikely that real name and identity used anyway.

Disclosure of Trade Secret or Proprietary Information

- *Apple Computer v. Doe 1, et al.*, 139 Cal. App. 4th 1423 (2006).
 - Court ordered an ISP to identify people Apple accused of stealing trade secrets and leaking information about Apple products through websites.
 - Court left unresolved the issue of whether the defendants were entitled to protection as journalists.

Unauthorized Use of Company Logos and Copyrighted Material

- *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.

Other Legal Risks

- Disclosure of nonpublic material or misleading information creating securities law issues
 - Regulation FD
 - SEC Rule 10(b)-5
 - Regulation G
- Damage to company's reputation and image based on conduct of employees
 - Employees posting videos on YouTube

Linked-In

- Should employers regulate giving references on LinkedIn?
- Unlawful solicitation of employees and customers
- E-discovery issues

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.

Contact Information



Renée T. Lawson
Litigation/eData
San Francisco
415.442.1443
rlawson@morganlewis.com



Melinda S. Riechert
Labor and Employment
Palo Alto
650.843.7530
mriechert@morganlewis.com



Carla B. Oakley
Intellectual Property
San Francisco
415.442.1301
coakley@morganlewis.com



James P. Walsh, Jr.
Labor and Employment
Princeton
609.919.6647
jwalsh@morganlewis.com



Howard M. Radzely
Labor and Employment
Washington, D.C.
202.739.5996
hradzely@morganlewis.com