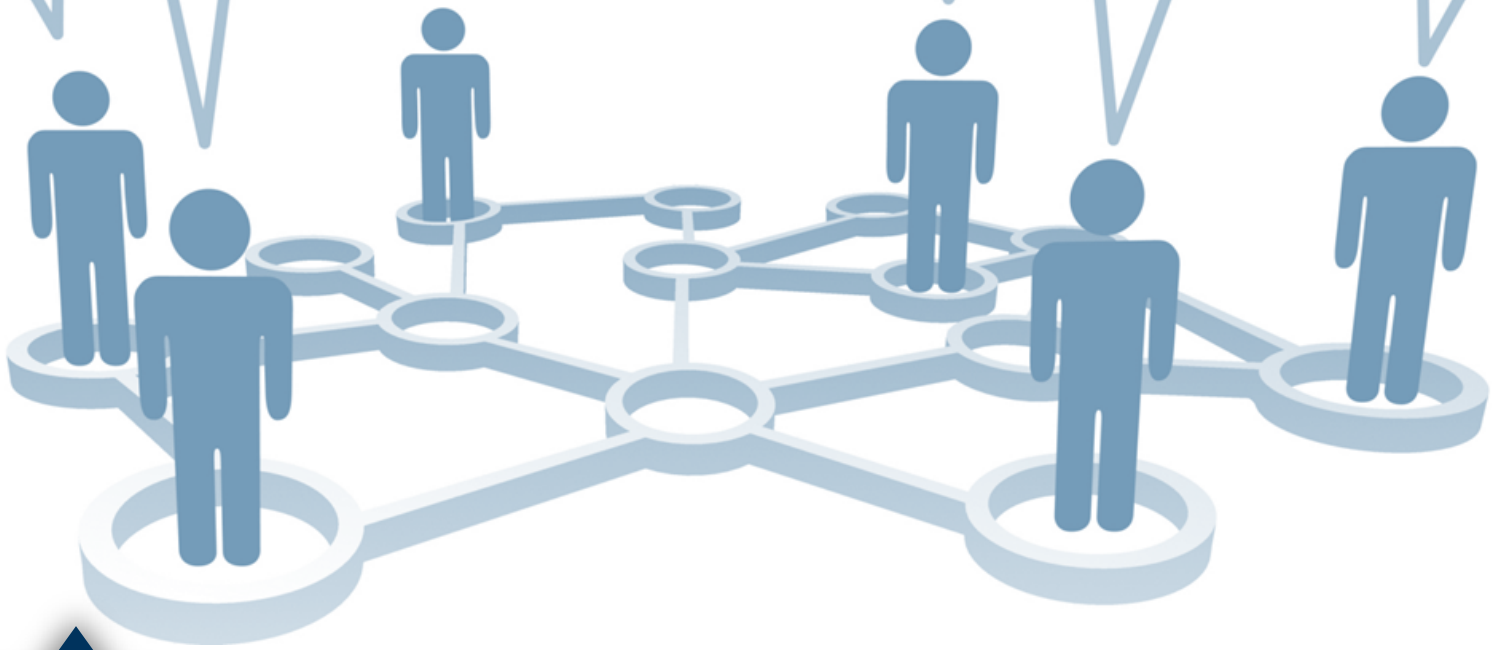
Social Media in the Workplace

Stacey L. Smiricky | Partner, Labor & Employment Group

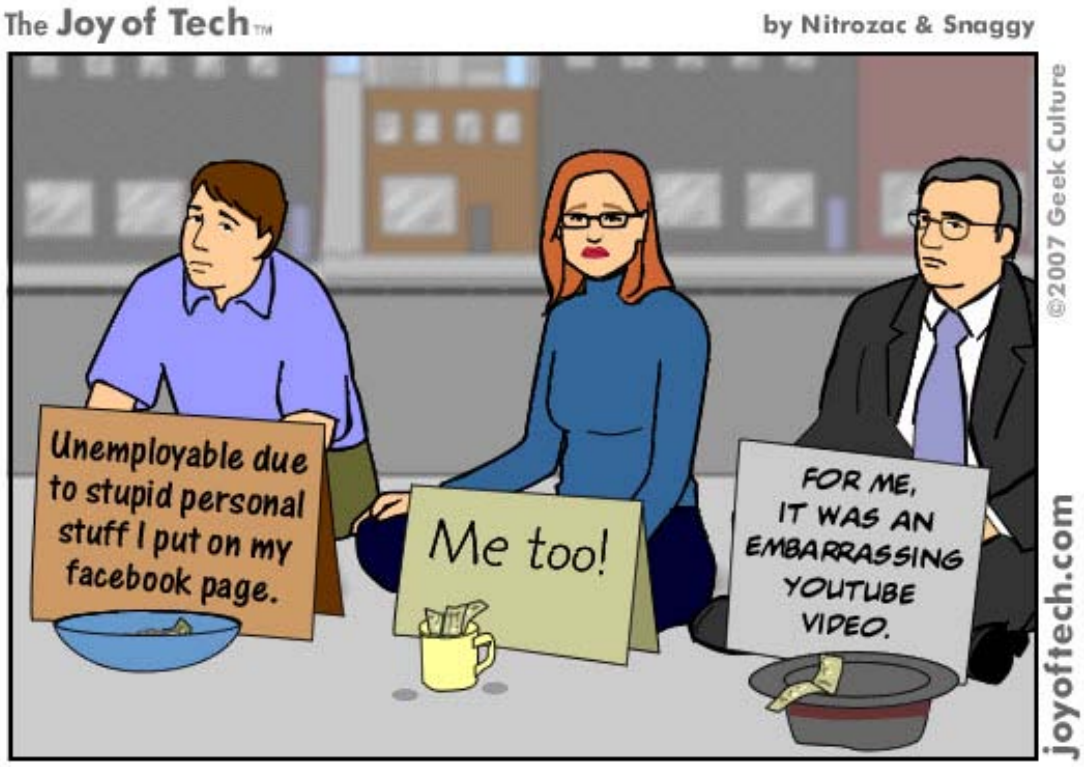


FAEGRE BAKER DANIELS

FAEGREBD Consulting

Lessons Learned

Employee who called in sick later places a status update on his Facebook page announcing “sick day” at Wrigley Field



Signs of the social networking times.

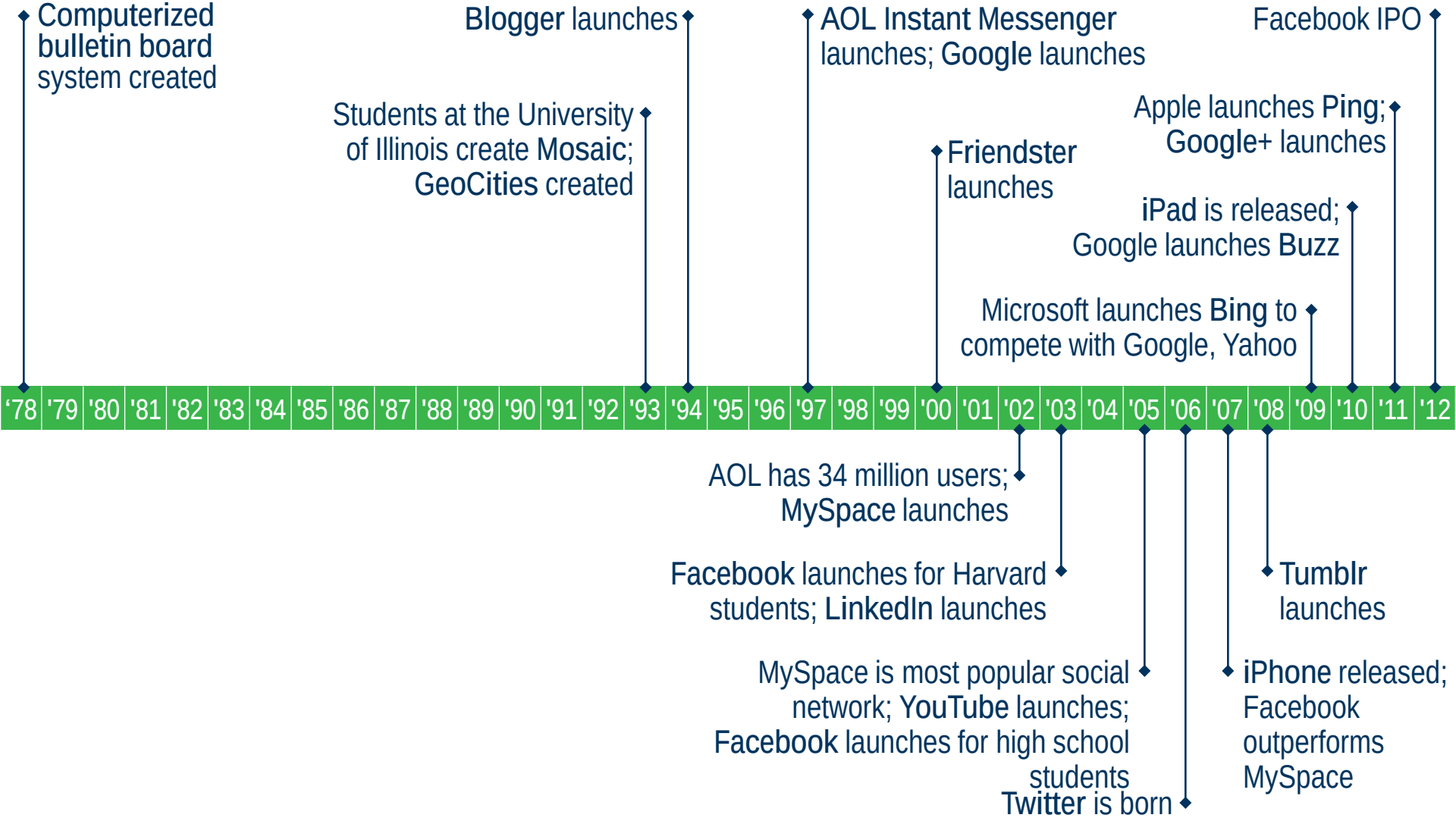
Why are we here?

Topics to be covered:

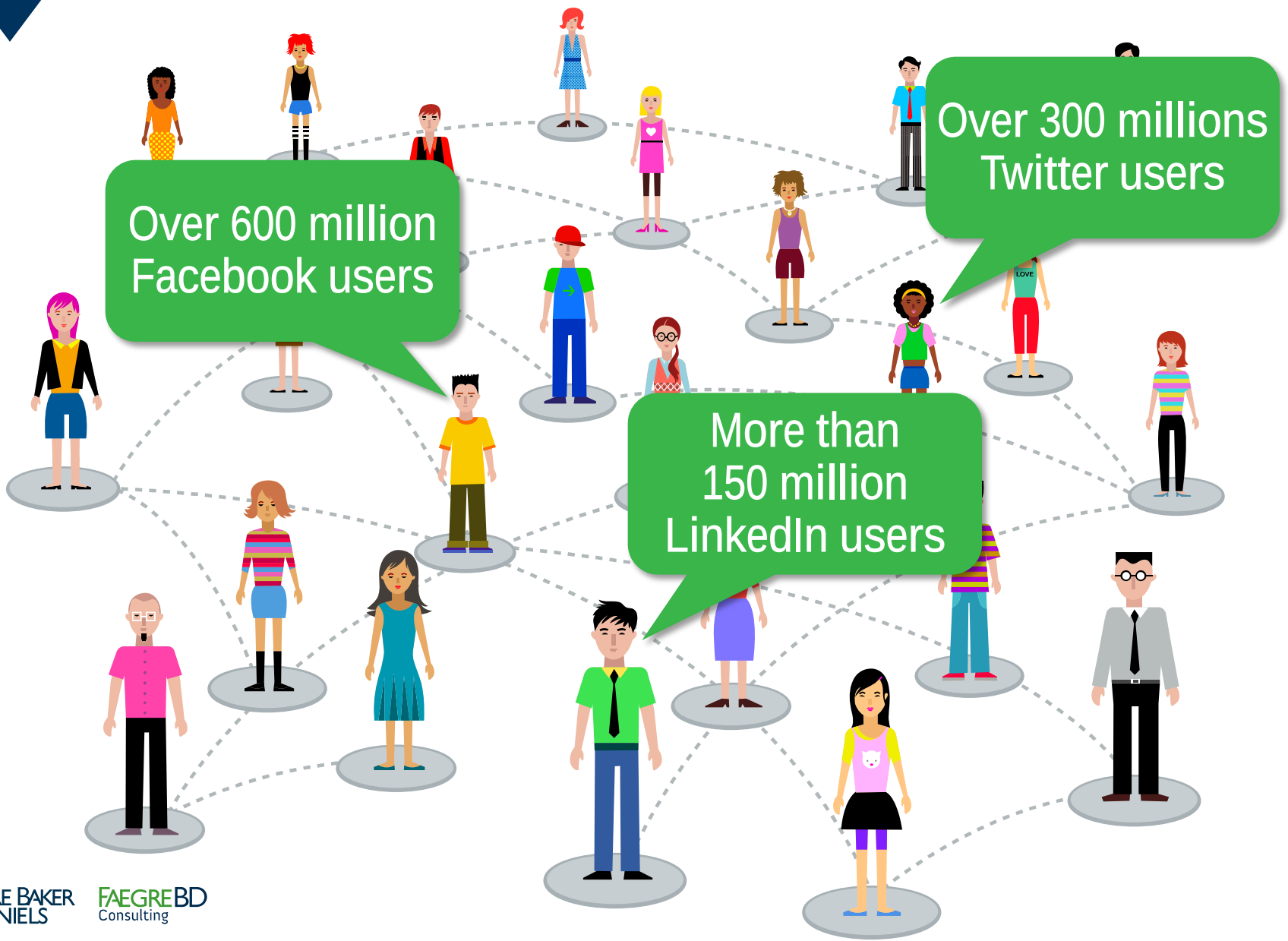
- Development of social media
- Business uses of social media
- Laws that affect use of social media in the workplace
- Company legal exposure due to use of social media
- Protecting the company

Development of Social Media

Social Media Timeline



Today


Over 600 million Facebook users
Over 300 millions Twitter users
More than 150 million LinkedIn users

Business Uses of Social Media

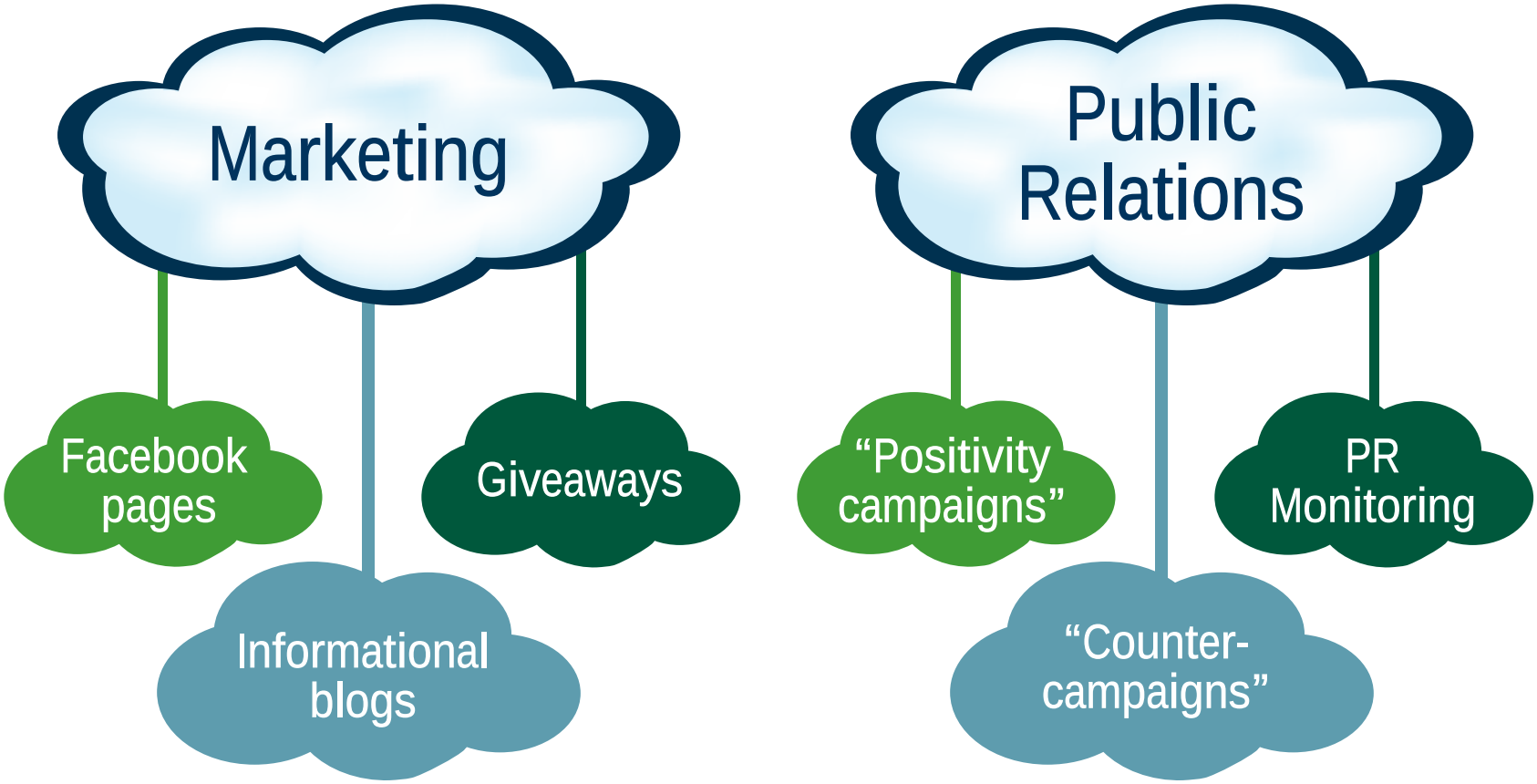
SHRM Survey

The Society for Human Resource Management (SHRM) recently released the findings of a social media survey they conducted. When asked if any groups or individuals in an organization currently engage in social media activities to reach external audiences, 68% of people surveyed replied with “yes”.

Some other interesting findings from the survey include:

- 31% of companies track employee use of social media services.
- 43% block access to social media platforms on company computers and handheld devices.
- The three most likely groups in an organization to use social media are marketing (67%), HR (44%) and public relations (38%).
- Only 27% of companies provide social media training to employees who engage in social media activities on behalf of the company.

How Are Businesses Using Social Media



How Are Employers Using Social Media

- Recruiting
- Employment candidate screenings
- Employee monitoring
- Litigation

Social Media in the Workplace: The Legal Issues

Potentially hundreds of federal and state laws could affect the use of social media in the workplace.

The ones getting the most attention are:

- The National Labor Relations Act
- The Fair Credit Reporting Act
- Anti-discrimination statutes such at Title VII, the Age Discrimination in Employment Act and the Americans with Disabilities Act
- General privacy rights under the First Amendment, Stored Communications Act or Federal Wiretap Act

The Big One

National Labor Relations Act ("NLRA"): Section 7 of the NLRA prohibits employers from enacting policies that stifle or prevent employees from engaging in "concerted activity" for "mutual aid and protection."

According to the NLRB, there are two main points to consider:

- Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
- An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

Fair Credit Reporting Act

- **The Fair Credit Reporting Act** requires a job applicant's or current employee's consent before the employer hires a third party to run background checks.

- Many background checks and third-party investigations now include social media searches. If these searches are performed and the proper consent not obtained, the employer could violate the FCRA and subject itself to civil penalties.

Anti-Discrimination Laws

- Employers conducting their own Google or Facebook search as part of employment decisions will normally obtain information about the candidate's protected characteristics on the user's profile page through photos, wall posts and affiliations.
- It is easy to picture a lawsuit for discrimination when a candidate is not chosen and the employer admits to having viewed the candidate's social media page that revealed a protected characteristic not present on the chosen candidate's page.

Privacy Concerns

An employer is permitted to monitor work-related use of electronically generated communications when the monitoring serves a legitimate business interest. Employers should be aware of privacy concerns when they monitor employees' electronic communications.

BUT REMEMBER:

- **The Wiretap Act:** Permits an employer to intercept electronic communications where there is a legitimate business reason for the interception. An employee's failure to restrict privacy settings will likely lead to legitimate viewing of his or her social media profile.
- **Stored Communications Act:** Congress passed the SCA to prevent communication providers from divulging private communications to certain entities and individuals. How does this affect employers?
  - **Pietrylo v. Hillstone Restaurant Group (D.N.J. 2009):** employer found liable under the SCA for coercing an employee to give it the password to a private MySpace page used by employees to complain about work conditions and then firing the page's creator.
- Employers could violate either the Wiretap Act or the Stored Communications Act by accessing private information.
- Public employers need to be wary of First Amendment concerns when monitoring employees' use of government-owned computers.

Employers Headaches from Social Media…

- *Maremont v. Susan Fredman Design Group, Ltd.*, 2011 U.S. Dist. LEXIS 26441 (N.D. Ill. Mar. 15, 2011) (employer allegedly impersonated employee on employee's Facebook and Twitter accounts)
- *Ade v. Kidspeace Corp.*, 698 F. Supp. 2d 501 (E.D. Pa. 2010) (fired employee sued employer for failing to discipline another employee for sending sexually explicit messages to a co-worker through MySpace)
- *Amira-Jabbar v. Travel Servs.*, Inc., 2010 U.S. Dist. LEXIS 76363 (D.P.R. July 28, 2010) (employee sued former employer based on discriminatory remark that another employee made on his Facebook "wall" with company computer during work time)
- *Nguyen v. Starbucks Coffee Corp.*, 2009 U.S. Dist. LEXIS 113461 (N.D. Cal. Dec. 7, 2009 (Starbucks employees expressed concern over their safety, based on threats that a co-worker made against them and Starbucks on MySpace)
- *Yath v. Fairview Clinics*, 767 N.W. 2d 34 (Minn. Ct. App. 2009) (suggesting that employer could potentially be liable for invasion-of-privacy claim based on an employee's posting of private information on MySpace)

Other Legal Issues:

Misappropriation and Conversion

An employee developed and maintained a Twitter account using his own identity in furtherance of his job working for an interactive news web resource. He developed a large Twitter following. When he was terminated, the company asked him to turn over the use of the Twitter account. The employee declined, changed his Twitter password and account name and continued to use the account. The company sued the employee for misappropriation of trade secrets, conversion, and interference with economic advantage. The case will ultimately address whether a Twitter account and its followers are protectable trade secrets.

Other Legal Issues:

- Social Media Content May Not Be Private Even With Privacy Settings
  - An individual sued for injuries sustained in a car accident including permanent physical injuries. On her Facebook page the individual posted status updates about exercising at a gym, and later made the page private. The court granted the defendant's motion to compel and required the individual to provide defense counsel with her Facebook password so defense counsel could view her page. The court stated, “By definition, there can be little privacy on a social networking website. Facebook’s foremost purpose is to ‘help you connect and share with the people in your life.’ That can only be accomplished by sharing information with others. Only the uninitiated or foolish could believe that Facebook is an online lockbox of secrets.”
  - This court’s opinion is similar to several other decisions that have held that privacy settings are unlikely to protect social media content from discovery.

Other Legal Issues:

- "Like" button may be enough to trigger NLRA rights
  - Three D LLC d/b/a Triple Play Sports (1/3/12 NLRB ALJ) required the administrative law judge to determine whether the NLRA protected an employee whose only involvement in an online employee discussion of a payroll tax withholding was to click the "Like" button on a Facebook page. Looking at the Facebook "wall" the ALJ found the employee engaged in concerted activity because the employee used the "Like" button to express approval of other employee complaints concerning payroll tax issues.

Upcoming Legislation

- **SOPA (Stop Online Piracy Act):** expands the ability of U.S. law enforcement to fight online trafficking in copyrighted IP and counterfeit goods. Provisions include the requesting of court orders to prohibit search engines from linking to sites that have infringing material and to prohibit advertising networks and payment facilities from conducting business with infringing websites. The law would expand existing criminal laws to include unauthorized streaming of copyrighted content.
- **PIPA (Protect Intellectual Property Act):** Senate version of SOPA.
- **Illinois Legislation:** Prohibits employers from using employees' personal passwords to access employees' personal email and social networking accounts.

The Downside: Legal Exposure from Use of Social Media

Social Media: Risks Created by Employee Use

- Disclosure of confidential or proprietary information of the company or customers.
- Disclosure of material inside information in violation of securities laws.
- Damage to brand, image or reputation of the company.
- Statements that are harmful, offensive, or inflammatory.
- Claims for negligent hiring or retention.
- Unauthorized statements or endorsements on behalf of the company.
- Wage/hour claims.

Social Media: Risks Created by Employer Monitoring

- Mistakes
- Bad publicity
- Violations of law
  - Fair credit reporting statutes
  - Lawful off-duty conduct statutes
  - Non-discrimination statutes
  - Privacy-related claims
  - Labor laws

How To Protect Your Business From Legal Exposure

Reducing Risk: Investigating Job Candidates

- Make a policy decision whether or not to conduct Internet searches of candidates.
- Establish search protocols and procedures and apply them consistently.
- Decide whether to use a consumer reporting agency and make appropriate disclosures.
- Provide EEO training for internal staff.
- Decide what candidates to search and when during the process.
- Search only publicly available information that is not password-protected.
- Consider appropriate, confidential documentation.
- Insulate the decision maker from impermissible considerations.
- Check your facts.

Reducing Risk: Monitoring Employees

- Apply the same considerations for all candidates and:
  - Seek legal advice regarding information that may be subject to attorney-client privilege.
  - Adopt a social media policy.

Social Media Policies:

- A comprehensive social media policy can minimize future costs by placing employees on notice as to what content and behavior is acceptable in using social media.
- Policy can serve as a foundation for future disciplinary action to be taken.
- Careful consideration must be given to the contents of a social media policy.
- It is important for employers to remember that there is no one policy that will work for every employer or avoid all risks.
- Employers should implement policies that describe social media and its uses and outline which activities are subject to the policy. The policy should outline when it is acceptable to use social media during work, if at all.
- When employees are allowed to make postings on behalf of the company, mandatory training and prior approval should be implemented. Employees should be advised they must use their real names and the company name when posting on the company's behalf. They should refrain from disparaging the company, its customers and vendors and from divulging any trade secrets or other information protected by the company's confidentiality provisions.
- The policy should also reference all other relevant policies, including the company's anti-discrimination/harassment policies, computer use policies and confidentiality policies.

Unlawful Policies

- The General Counsel of the NLRB found to be unlawful:
  - A social media policy that provided no guidance on what constituted the prohibited “inappropriate postings” on social media sites. The NLRB felt that this allowed employees to reasonably interpret the rule to prohibit protected concerted activities.
  - A work rule prohibiting “inappropriate conversation,” whether in person or online, was unlawful when it provided no guidance on what constituted the prohibited “"inappropriate conversation.”
  - A company policy that prohibited employees from disclosing or communicating information of a confidential, sensitive, or non-public nature using company resources to those outside the company was unlawful when it failed to give examples of such violations.
  - Two policies prohibiting employees from making disparaging comments about the company or from engaging in unprofessional conduct online were found to be unlawful when the NLRB felt such policies “would reasonably tend to chill employees in the exercise of their Section 7 rights.”

Lawful Policies

- The NLRB found lawful a policy that prohibited the use of social media to post or display comments about co-workers, supervisors, or the employer that were vulgar, obscene, threatening, intimidating, harassing, or in violation of the employer's anti-discrimination and anti-harassment policies. The NLRB stated that forbidding "statements which are slanderous or detrimental to the company" that appeared on a list of prohibited conduct including "sexual or racial harassment" and "sabotage" would not be reasonably understood to restrict Section 7 activity."
- The NLRB also found lawful a policy that required employees to confine their social networking to matters unrelated to the company if necessary to ensure compliance with securities regulations and other laws. The NLRB stated that employees would reasonably "interpret the rule to address only those communications that could implicate security regulations."
- The NLRB also found lawful that company's policy prohibiting employees from using or disclosing confidential and/or proprietary information, including personal health information about customers and patients. The NLRB stated that "employees would reasonably understand that this rule was intended to protect the privacy interests of the Employer's customers and not to restrict Section 7 protected communications."

Implementing the Social Media Policy

- While developing and drafting a social media policy is a good start, a policy is not complete without adequate training and education of employees. Simply drafting a policy and inserting it into an employee handbook is not enough. To be effective, the policy should be communicated directly to employees.

- The most effective communication will be through speaking directly with employees. Create an open forum where social media issues are discussed. Educate employees on the fact that content posted on the Internet will remain on the Internet for a long time. While many people may understand the permanency of Internet posts, some employees may not. Taking the time to educate and discuss can go a long way toward protecting the company.

Enforcement

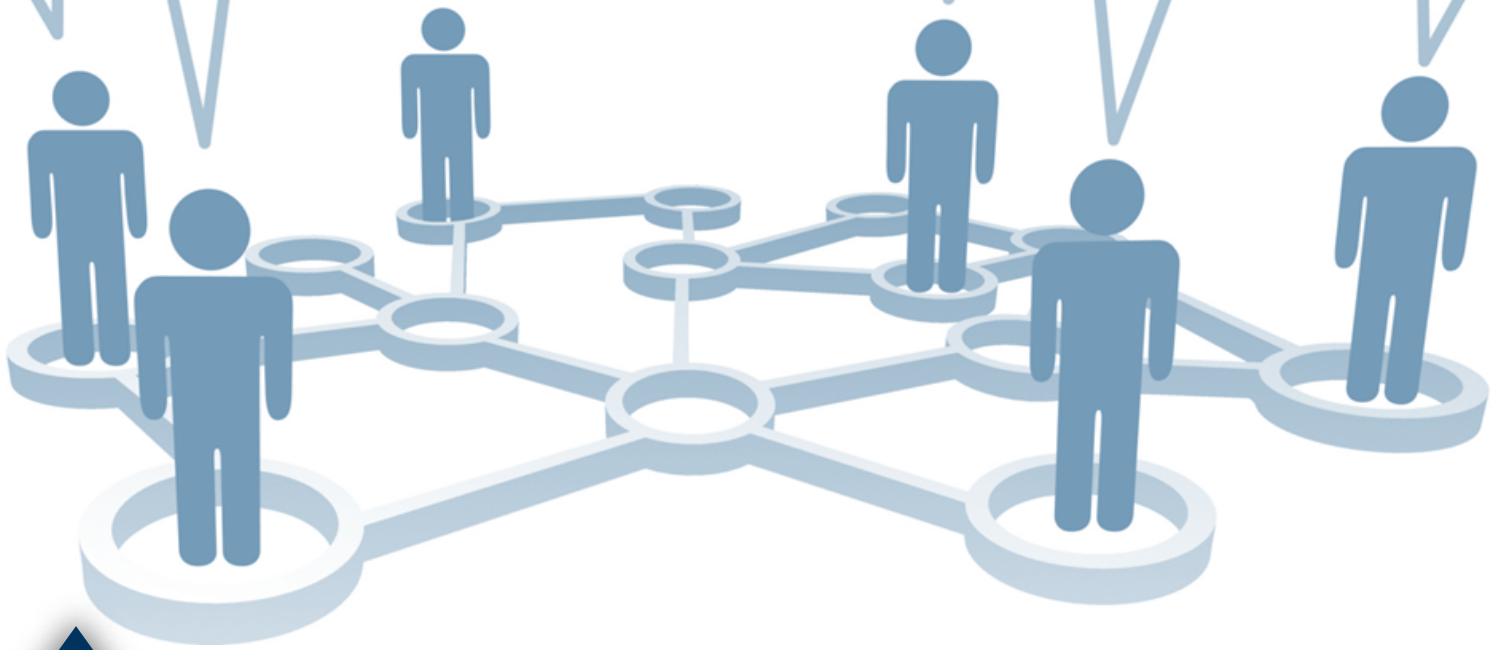
ENFORCE THE POLICY…

CONSISTENTLY!

Questions?

Social Media in the Workplace

Stacey L. Smiricky | Partner, Labor & Employment Group



FAEGRE BAKER DANIELS

FAEGREBD Consulting