SOCIAL MEDIA IN THE WORKPLACE

Emerging Issues

• KELLY ANN BIRD
  FEBRUARY 15, 2017
INTRODUCTION

- As of June 2016, Facebook had over 1.13 billion daily active users
  - 71% of online adults use Facebook
    - 58% of Facebook users say they are connected to work colleagues
- Twitter had 313 million monthly active users and 1 billion monthly unique visits to sites embedded in Tweets
  - Over 982 million existing Twitter accounts
    - 500 million “tweet” status updates and messages per day
- Snapchat had 150 million daily users as of June 2016
CONCERNS?

- Reduced productivity
  - 34% use social media to take a mental break from their job
  - 27% connect with family and friends while at work
- Leaking confidential information and/or trade secrets
- Posting defamatory, offensive, or inappropriate comments
- "Cybersmearing"
ROADMAP

• Do you have a compliant social media policy?
• What are the limits to restricting employees’ social media activities?
• Social media risks in recruiting, hiring and firing
• What about personal devices?
POLICIES

• Legal Barriers
  – NLRA
  – State laws

• Your company’s/client’s priorities, values, and ability to administer

• Guideposts

• Change ahead?
THE “NEW” NLRA

Section 7

- protects the right of employees to take “concerted” action for their “mutual aid or protection” regarding “terms and conditions” of employment.

- generally applies to all employees including those privately employed.
NLRB ACTIVITY

- Common provisions found in employer policies subject to scrutiny.
- Are employee social media posts “protected concerted activity”?
- Does discipline or policy violate the NLRA?
PROBLEMATIC POLICIES

• Per NLRB, violation of NLRA if policy is overly broad and reasonable interpretation does not exclude Section 7 activity.
  
  – *Costco Wholesale Corp.*, 352 NLRB No. 106 (Sept. 7, 2012)
  – *Knauz BMW*, 358 NLRB No. 164 (Sept. 28, 2012)
CHECKLIST FOR POLICIES

– Would employees reasonably construe the language to prohibit Section 7 activity;
– Was the rule promulgated in response to union activity; or
– Has the rule been applied to restrict the exercise of Section 7 rights?
QUIZ #1

“If you aren't careful and don't use your head, your online activity can also damage [the Company] or spread incomplete, confidential, or inaccurate information. … You may not make disparaging, false, misleading...statements about or relating to [the Company], our employees, suppliers, customers, competition, or investors.”
CHIPOTLE

- The NLRB affirmed the ALJ
- The policy violated the NLRA on two separate grounds
  - The term “confidential” was undefined and employees could reasonably understand it to encompass matters protected by Section 7, such as compensation and benefits.
  - The prohibition on “false” or “disparaging” statements was overbroad because false statements are protected unless they are maliciously false, i.e., knowingly or recklessly false, and employees’ right to make derogatory statements about the terms and conditions of employment is also protected.

Chipotle Services LLC d/b/a Chipotle Mexican Grill & Pennsylvania Workers Org. Comm., A Project of the Fast Food Workers Comm, 364 NLRB No. 72 (Aug. 18, 2016)
QUIZ #2

Employees are prohibited from “making disparaging or defamatory comments about the company, its employees, officers, directors, customers, partners, or its products and services.”
DISH

• The NLRB upheld the ALJ’s ruling
  – social media policies are invalid if employees reasonably could interpret them to chill their rights to organize

Dish Network Corp. & Commc’ns Workers of Am., Local 6171 & Eric Sutton
OTHER UNLAWFUL PROHIBITIONS

- Do not make “insulting, embarrassing, hurtful or abusive comments about other company employees online”
- “Avoid the use of offensive, derogatory, or prejudicial comments.”
- Do not “[e]mail, post, comment or blog anonymously. You may think it is anonymous, but it is most likely traceable to you and the [c]ompany.”
- Do not “[c]reate a blog or online group related to your job without the advance approval of the” legal and communications departments.
LAWFUL RESTRICTIONS

• “Do not make negative comments about our customers in any social media”
• You may not “[c]reate a blog or online group related to [the company] (not including blogs or discussions involving wages, benefits, or other terms and conditions of employment, or other protected activity) without the advance approval of the legal and communications department.”
• “Do Not Violate the Law and Related Company Policies: Be thoughtful in all your communications and dealings with others, including email and social media. Never harass (as defined by our anti-harassment policy), threaten, libel or defame fellow professionals, employees, clients, competitors or anyone else. In general, it is always wise to remember that what you say in social media can often be seen by anyone. Accordingly, harassing comments, obscenities or similar conduct that would violate [company] policies is discouraged in general and is never allowed while using [company] equipment or during your working time.”
• “If you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying.”
CHANGE IN SIGHT?

• Trump administration will name three of the five members of the NLRB, and after next year, will also appoint the all-important general counsel, who decides which cases are heard by the board.
• Mid-2017 is most likely the earliest any change will take place.
RESTRICTING ACTIVITIES

• Desirable?
  – Why?

• Possible?
  – How?
  – Legal minefields?

• Enforceable?
  – Can you?
  – Will you?
EMPLOYER POLICIES

• A well-drafted policy should:
  – place employees on notice as to what content and behavior is acceptable in using social media
  – outline when it is acceptable to use social media during work (if the company allows for such)
  – reference the Company’s other relevant policies such as non-discrimination and anti-retaliation, acceptable computer use, and confidentiality policies
  – Identify potential repercussions for policy violations

• The Company should provide training for employees, including those who will post on behalf of the Company
HIRING AND FIRING

• What role does social media play?
• Research
  – How?
  – Who?
  – Legal restrictions?
  – Legal risk?
• Action
WHO USES SOCIAL MEDIA?

- According to a 2016 survey of over 2,000 hiring managers and more than 3,000 workers:
  - 60% of employers use social networking sites to research job candidates
  - 59% of hiring managers use search engines to research candidates

- Of those employers who research job candidates on social networking sites
  - 49% found content that caused them not to hire the candidate
  - 32% found content that made them more likely to hire a candidate
SOCIAL MEDIA HAZARDS

• Legal Risks
  – Privacy Issues
  – Asking candidates to provide access/passwords

• Problem of too much information
  – Discrimination
  – Activities protected by National Labor Relations Act
  – State legal activities laws
  – First Amendment for public employees
SKIP THIS STEP?

- Negligence
- Knowledge
- Fact-checking
MAYBE JUST OUTSOURCE?

• Fair Credit Reporting Act compliance
  – “credit reporting agency”
  – authorization and disclosures required
  – copy of report
  – notice re adverse action
BEST PRACTICES

– Policy and protocol controlling access to social media sites
  • Screen applicants in a uniform manner
  • Create a list of the social media to be searched for each applicant
  • Determine what types of lawful information to obtain
  • Only search for job related information
  • Only search public sites
  • Do not “friend” applicants in order to gain access to their nonpublic social networking profiles

– Train managers and human resources staff
– Keep decision makers out of the process
– Conduct search after interview or make contingent offer
– Get employee authorization
– Consider third party vendor
SOCIAL MEDIA TERMINATIONS

• What is posted?
• How did the employer learn about it?
• Is the posting protected?
  is it concerted activity or individual griping?
  • Does posting seek to initiate, induce or prepare for group action?
  • Does the posting reference, involve or concern wages, hours, benefits, working conditions or other terms and conditions of employment?
  • Does posting reference conversations with coworkers that occurred before postings were made so that posting is a logical outgrowth of those conversations?
  • Does posting seek to bring truly group complaints to the attention of management?
  • Are any co-workers of the employee posting Facebook friends or Twitter (or other blog) followers?
  • Did any co-worker respond to the online post?
  • If so, what was the nature of that response?
• Was conduct so outrageous as to lose protection of the NLRA?
PERSONAL DEVICES AND BYOD

• What do your employees use all day?
• Why?
• What can they access?
• What protections does your company need?
A DISRUPTIVE PHENOMENON

“Bring your own device, or BYOD, is a disruptive phenomenon where employees bring non-company IT into the organization and demand to be connected to everything – without proper accountability or oversight.”

Source: [http://www.gartner.com/technology/topics/byod.jsp](http://www.gartner.com/technology/topics/byod.jsp)
“Sensitive information on the device may be stored alongside personal videos of junior league soccer and Angry Birds, which the employee’s 4-year-old daughter plays daily. One mis-swipe, or wrong button hit, and the work data could be corrupted, lost or accidentally transmitted to the entire junior league.”

PERSONAL DEVICE PROBLEMS

- Constantly changing data map
- Tracking devices AND data they access
- Technical hurdles/impediments for litigation holds and data collection
- Does employer have “possession, custody or control”?
- Third parties
- Former employees
PRIVACY ISSUES

- CFAA and SCA
- HIPAA/GINA
- FCRA
- State laws
- International Laws
EMPLOYEE CONSIDERATIONS

- Weigh convenience/efficiency against privacy concerns
- Consider carrying two devices – work and personal
- Demand detailed written policy that strictly limits GPS tracking and “viewing” to stated business purpose
- Read the policy!
- Back up all personal files, photos, music
BYOD POLICIES

- Define the Scope
- Define Appropriate Use
- Define Cost and Support
- Implement Security Protocols
- Consequences for Violations
- Monitoring Access
- Monitoring Use
- Training
QUESTIONS?