WELCOME

Welcome to the K&L Gates webinar presentation. Audio for this event will be heard over the web. Please turn on your speakers or adjust your audio level to hear the presentation. In the panel located above the chat window called "Audio Information," press the > button and confirm that it reads "Connected" to hear the audio for this presentation. You will hear music until the start of the presentation.

To submit questions for the presenters, please enter your question in the “Chat with Presenter” window located at the bottom left corner of your display. Slides for this program will be made available after the program. Thank you.
March 31, 2015

Social Media in the Workplace

Mark S. Filipini, Partner, K&L Gates (Seattle)

Michael A. Pavlick, Partner, K&L Gates (Pittsburgh)
AGENDA

- Applicants and Social Media
- Social Media and the NLRB
- Confidentiality and the NLRB
- Astroturfing – Social Media
- Social Media and Litigation
Applicants and Social Media
APPLICANTS AND SOCIAL MEDIA

- Employers may check an applicant on Facebook, LinkedIn, Twitter, etc.
  - NYT (2011): 70% of recruiters denied employment because of information found online
  - SHRM: 76% of companies use/plan to use social media for recruiting
- Practice is not illegal by itself, but . . .
  - Has the employer accessed the account legally?
  - Has the employer accessed information that it should not have?
USE OF SOCIAL MEDIA FOR SCREENING

- Social media can reveal information of legitimate interest to employer
  - Communications skills and creativity
  - Truth of stated qualifications
  - Posted inappropriate comments or engaged in inappropriate activity
  - Criticized a former employer
  - Divulged confidential information
  - Rewards and accolades
  - Recommended by peers
USE OF SOCIAL MEDIA FOR SCREENING

- But social media information may be unreliable and unverifiable
- Also the risk that a search will disclose protected information
  - Age
  - Gender
  - Race
  - Religion
  - Medical information
SIMPLE REALITY

- Once information is learned, it cannot be unlearned
- Once information is learned, employer has to be able to explain how it used that information or why it did not use that information
EXAMPLE

- On Facebook page, Joe Sixpack refers to a Lung Cancer survivor group meeting
- If Employer refuses to interview Joe Sixpack, does it open itself to a claim that it has discriminated against Joe (and possibly a class of similarly situated applicants)
  - Because Joe is disabled under the ADA, e.g., has lung cancer, had lung cancer, or is perceived as having lung cancer, or
  - Because Joe is a smoker (some states protect smoking off the job)
EXAMPLE

- Mary’s resume shows that she has worked for non-union employers in manufacturing positions.
- On her Facebook page, there is a picture of her wearing a Teamsters t-shirt at a Labor Day parade.
- If the non-union company she applied to declines to offer her employment, can Mary file an unfair labor practice charge?
EXAMPLE

- Company searches social media for information about job applicant and finds none
- Company elects not to hire job applicant
- Does Company open itself to age discrimination claim because it could be argued that lack of social media footprint suggests individual is old and unable to adapt to change
  - Pew (2014): 46% of Americans 65 and older use social media while national average is 73%
HOW DO EMPLOYERS SCREEN

- Requesting usernames and passwords from applicants
- Retaining a third party vendor to review applicants’ social media presence
- Do It Yourself (DIY)
- Each method raises different issues and concerns
APPLICANT SCREENING AND ACCESS TO EMPLOYEE SOCIAL MEDIA ACCOUNTS

- State Password Protection Laws – generally two categories of restrictions
  - Specific restrictions on employer actions [13 States] - Employer may not require request, suggest, or cause employees or applicants to do any of the following:
    - Disclose a username or password;
    - Add an employee, supervisor, or administrator to employee’s contacts;
    - Change privacy settings;
    - Access personal social media in the presence of the employer.
  - General “gain access restrictions” [5 States]
    - Employer may not require employees or prospective employees to provide any password or related account information to gain access to the individual’s account or profile on a social networking website (also referred to as personal accounts or services).
- Prohibitions generally prohibit retaliation against applicants and employees who fail to provide their social media information to the employer
APPLICANT SCREENING AND ACCESS TO EMPLOYEE SOCIAL MEDIA ACCOUNTS

- Exceptions
  - Employer Related Social Media Accounts
  - Employee’s Personal Email Address
  - Public Information
  - Legal Compliance
  - Employer Investigation of Misconduct
  - Inadvertent Receipt of Information
  - Workplace Policies: Generally not prohibited from adopting or enforcing lawful workplace policies governing the use of employer’s electronic devices or monitoring
USE OF THIRD PARTY VENDORS

- Companies can be retained to provide social media screening reports on applicants and employees
- Such reports are considered to be consumer reports under Fair Credit Reporting Act (FCRA)
- FCRA creates various obligations for the employer and rights for the applicant or employee
FAIR CREDIT REPORTING ACT

A credit reporting agency may provide information to employer about person if:

- Person is informed in writing that a background check may be obtained
- Person authorizes check in writing (on separate form)
- If employment is denied on basis of check, person must be provided:
  - Copy of report
  - Statement of rights under FCRA
  - Opportunity to explain adverse information prior to decision
DO IT YOURSELF

- Discrimination issues
- Negligent hiring/retention
- Screening unreliable or unverifiable information
BEST PRACTICES

- Respect privacy
  - Unauthorized access, hacking, deceptive practices
    - Stored Communications Act – prohibits intentional access of electronic communications services without authorization
    - Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002);
  - Password laws
  - Search only public content
  - Comply with terms of service for each site visited
BEST PRACTICES

- Be aware of FCRA requirements
  - FCRA type notification for social media searches even if not covered by FCRA
    - Reference social media in standard authorization on application
- Document employment/hiring decisions
- Search social media in a uniform manner
  - Visit same sites or have concrete reason for variances
BEST PRACTICES

- Mitigate discrimination claims
  - Employers who learn about protected characteristics via social media cannot claim ignorance as a defense
    - *Gaskell v. Univ. of Kentucky*, 2010 WL 4867630 (E.D. Ky. 2010) (summary judgment motion denied because employer learned of candidate’s religious beliefs through online investigation)
  - Separate the screener from the decisionmaker
    - Designate a researcher who reviews background materials like social media and have researcher “scrub” the materials of any reference to protected activities or characteristics
    - Importance of training
BEST PRACTICES

- Search social media post-interview or even post-offer
- Employ a healthy dose of skepticism
  - Verify information or find additional supporting information
  - Use multiple sources
  - Follow-up if necessary
Social Media and the NLRB
NATIONAL LABOR RELATIONS ACT (NLRA)

- Federal law recognizing private sector employees’ right to join or not join a union.
  - Broad definition of “employee”
- Section 7 – “Employees shall have the right …to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection....”
- Interpreted and enforced by the National Labor Relations Board (NLRB)
  - Investigates and prosecutes unfair labor practices
  - 5-member Board interprets and applies law
PROTECTED CONCERTED ACTIVITIES

- Section 7 rights extend to all employees covered by the NLRA, whether or not they are represented by a union.
- Some examples: organizing efforts (including informal meetings, solicitations, distributing information), discussion about pay and benefits, complaints to or about management regarding working conditions.
PROTECTED CONCERTED ACTIVITIES – SOCIAL MEDIA

- NLRA has long safeguarded employee speech regarding terms and conditions of employment
  - Be careful before disciplining for “insubordinate” comments or behavior
    - Is it “protected” and “concerted”?

- Existing protections apply to social media
  - Nature and spread of social media has reinvigorated NLRB, but significant precedent exists in Board and appellate decisions
  - Bottom line – don’t bet on issue going away
PROTECTED CONCERTED ACTIVITIES – SOCIAL MEDIA

- Protected = Speech (whatever the medium) or action regarding terms and conditions of employment or working conditions
- Robust right
  - Time, place and manner restrictions exist in case law but are limited
    - Presumption favors protection
    - Complaints to clients/customers generally OK
    - Social media lends itself to online gripes, gossip and questions regarding terms and conditions, including complaints about coworkers and supervisors
PROTECTED CONCERTED ACTIVITIES – SOCIAL MEDIA

- Collaborative nature of social media also lends itself to “concerted” activity label

- Concerted activities include:
  - Joint complaints, requests or discussions (i.e., 2 or more active employees)
  - Relaying information from prior joint sessions
    - “On the authority” of other employees
  - Actions that precede or attempt to initiate, induce or prepare for group action, including preliminary discussions of shared concerns
  - Appeals to third parties
SOCIAL MEDIA AND THE NLRB

- NLRB aggressively examining and finding fault with employer social media policies
  - All segments of private industry
    - Many non-unionized employers and some unions
  - Growing – and sometimes conflicting – body of advice and examples
    - Initiative by NLRB Office of the GC
    - Individual ULP cases
      - 3 Advice Memorandums
      - Numerous NLRB and ALJ Decisions
      - Appeals process likely to end up at Supreme Court
SOCIAL MEDIA AND THE NLRB

- Common pitfalls in social media policies
  - Prohibitions against insubordinate, disrespectful, damaging, disparaging or malicious comments
    - Distinguished from discriminatory, harassing, violent, threatening or libelous remarks
  - Restricting right to communicate regarding terms and conditions, including pay and discipline
    - Section 7 rights generally trump privacy concerns
  - Prohibiting employees from commenting on employer’s official web presence(s)
    - But employer controls its “official” voice
SOCIAL MEDIA AND THE NLRB

- Common pitfalls (cont’d)
  - Restricting contact with third parties, including government agencies, media and customers or clients
  - Prohibiting comment on pending litigation or administrative complaints
  - Limiting employees’ rights to “friend” each other
    - Distinction *should* be drawn with management
  - Requiring employees to police each other’s social media conduct
  - Protecting company’s reputation or integrity
    - Disparaging company’s product (un-protected activity) v. working conditions (protected activity)
SOCIAL MEDIA AND THE NLRB

- Common pitfalls (cont’d)
  - Prohibiting posting of photos or videos involving co-workers or working conditions
  - Prohibiting disclosure of confidential information
    - Red flag words: personnel, employees, co-workers, colleagues, employment terms or conditions, pay practices, benefits, policies
  - Prohibiting all use of trademarks or logos
  - Dire warnings
  - Requiring prior permission from HR, Legal or anyone else
SOCIAL MEDIA AND THE NLRB

- Best practices in a social media policy
  - Avoid or limit blanket prohibitions
    - NLRB often finds language is “overbroad”
  - Be as clear as possible
    - NLRB also often finds language is “ambiguous”
    - Ambiguous and/or overbroad = chilling effect
  - Reference and rely upon other policies
    - EEO, anti-harassment, Code of Conduct, etc.
SOCIAL MEDIA AND THE NLRB

- Overbroad Policies that Chill Section 7 Rights
  - “Don't pick fights. Social media is about conversations. When engaging with others online, adopt a warm and friendly tone that will encourage others to respond to your postings and join your conversation.”
  - “No one should be disrespectful or use profanity or any other language which injures the image or reputation of the (employer).”
  - “(Employer) prohibits any communications that are obscene, harassing, discriminatory or inflammatory.”
  - “You may not make disparaging or defamatory comments about (employer), its employees, officers, directors, vendors, customers, partners, affiliates or our, or their, products/services.”
  - “[I]t is important that employees practice caution and discretion when posting content [on social media] that could affect [the Employer's] business operation or reputation.”
SOCIAL MEDIA AND THE NLRB

- Best practices (cont’d)
  - Prohibitions should be specific (e.g., harassment and threats of violence)
  - Insert appropriate carve outs
    - Not enough alone to save overbroad policies, but necessary in policy itself
    - General and specific
    - Avoid fancy words or explain them – NLRA, Section 7, concerted activity
    - Possible alternatives – right to discuss terms and conditions, right to discuss working conditions, rights under federal labor law
  - Enforce policy wisely – often best to let comments pass or to respond politely
SOCIAL MEDIA AND THE NLRB

- Losing Protected Status
  - High standard
  - Disloyalty – publicly disparage products or services
  - Statements made with either the knowledge of their falsity or with reckless disregard for their truth or falsity
  - Harsh language and expletives insufficient
Confidentiality and the NLRB
CONFIDENTIALITY AND THE NLRB

- Many employers have one or more policies preventing disclosure of confidential information
  - Employee handbook
  - Individual agreements
    - IP protections
    - Restrictive covenants
  - Compensation plan documents
    - Stock or options
    - Bonuses
CONFIDENTIALITY AND THE NLRB

- NLRB’s social media initiative is sweeping in confidentiality policies
  - Obtained through employee filing ULP charge
  - Obtained via investigative process
  - Obtained via subpoena

- Board focuses on confidential information policies even if underlying ULP has nothing to do with it

- Primary problems – (1) directly in violation of law; (2) chilling Section 7 rights as overbroad and/or ambiguous
Language that failed NLRB examination:

- “Don’t release confidential guest, team member or company information….”
- “Employees are prohibited from posting information…that could be deemed material non-public information or any information that is considered confidential or proprietary.”
- “[y]ou shall not disclose…any information related to or concerning [Company X] that is not readily or easily available to the public….”
- “[e]mployees may not blog, enter chat rooms, post messages on public websites or otherwise disclose [employee records] that is not already disclosed as a public record.”
CONFIDENTIALITY AND THE NLRB

- Language that failed NLRB examination (cont’d):
  - “If during the course of your work you create, receive or become aware of personal information about (X’s) employees . . . don't disclose that information in any way via social media or other online activities.”
  - “[a]ll [personal employee] information must be held strictly confidential and cannot be disclosed to any third party for any reason . . . employees shall refrain from discussing private matters of member and other employees . . . includ[ing] . . . sick calls, leaves of absence, FMLA call outs, ADA accommodations, workers’ comp injuries, personal health information, etc.”
CONFIDENTIALITY AND THE NLRB

- Best practices for confidentiality policies
  - Provide specific examples
    - “Maintain the confidentiality of [Employer] trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential information.”
CONFIDENTIALITY AND THE NLRB

- Best practices (cont’d)
  - But Board rejected this
    - “Such information includes, but is not limited to, company performance, contracts, customer wins or losses, customer plans, maintenance, shutdowns, work stoppages, cost increases, customer news or business related travel plans or schedules.”
  - Take away – don’t list any work conditions in examples of confidential/proprietary information
CONFIDENTIALITY AND THE NLRB

- Best practices (cont’d)
  - Insert a carve out directly into each confidential information policy or rule
  - Address confidential information in the social media policy by a reference to specific policies addressing topic
EMAIL AND THE NLRB

Purple Communications (December 11, 2014)

- “[E]mployees who have rightful access to their employer’s email system in the course of their work have a right to use the email system to engage in Section 7-protected communications on nonworking time.”
- “In the course of their work” and “non-working time”
- “Special Circumstances”
- Business-only policies must be modified
- Potential effect on Social Media Policies
Astroturfing – Social Media
ASTROTURFING – SOCIAL MEDIA

- Failure to disclose that an individual is an employee of a company when he or she provides an online “consumer” review that:
  - Positively reviews that company’s own product
  - Negatively reviews a competitor’s product
  - Positively reviews a companion product (e.g. videogames that are only compatible with the employer’s specific gaming device)

- Legal Implications
  - FTC Regulation 16 C.F.R. § § 255.1, 255.5
  - False Advertising/Unfair Competition under the Lanham Act (and state laws regarding unfair competition)
  - Common law defamation
ASTROTURFING – SOCIAL MEDIA

FTC Regulations

- 16 C.F.R. § 255.1: Endorsements must reflect the honest opinions, findings, beliefs, or experience of the endorser.

- 16 C.F.R. § 255.5: When there exists a connection between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement (i.e., the connection is not reasonably expected by the audience), such connection must be fully disclosed.


(a) (1) Any person who, on or in connection with any goods or services, ... uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any ... false or misleading description of fact, or false or misleading representation of fact, which—

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.
ASTROTURFING – SOCIAL MEDIA

- Best Practices for Astroturfing Provisions in Social Media Policies
  - Create a comprehensive policy that addresses all forms of social media activity, including consumer review sites.
    - Discourage dishonest or misleading postings on social media about the company’s products/services or its competitors’ products/services. Be sure that this language is **narrowly drafted** and cannot be construed to discourage protected activity (e.g. criticisms of terms and conditions of employment).
    - If employees are going to post reviews, **require that they identify themselves in the review** as an employee of the company if the review relates to the company’s products/services, a competitor’s products/services, or products/services related to the company’s products or services.
  - Communicate the policy to employees and enforce it.
- Be proactive about false reviews of your own company; if you suspect someone has posted a false review, contact the site where it is posted and request it be removed. Review the site’s terms of use to determine if false reviews are a violation.
Social Media and Litigation
SOCIAL MEDIA AND LITIGATION

- Are a plaintiff’s social media activities discoverable and admissible?
- Value of informal discovery
  - Conduct informal discovery first
  - Allows you to propound specific discovery requests which will be less objectionable
    - But, is this surveillance under NLRA?
    - Possible ethical violations if obtained through false pretenses or without full disclosure of purpose for informal discovery
DISCOVERABILITY OF SOCIAL MEDIA

- **FRCP Rule 34(A)(1)(a)**
  - "electronically stored information"
  - "data compilations stored in any medium from which information can be obtained"

- **Advisory Committee Notes**
  - "Rule 34(a)(1) is expansive and includes any type of information that is stored electronically"
  - "The rule covers…information “stored in any medium,” to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."
DISCOVERABILITY OF SOCIAL MEDIA

- Within User's Custody and Control
  - Facebook: "you own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."

- Privacy Protections
  - FRCP 26(c)(1): "the court may…protect a party or person from annoyance, embarrassment, oppression…"
  - Federal or State laws
DISCOVERY STANDARDS

- Basic standard is relevance
  - Reasonably calculated to lead to discovery of relevant evidence
- Relevancy often demonstrated by showing that publicly accessible information on social media sites contradicts or controverts plaintiff’s claims or defenses.
- Alternatives ways to demonstrate relevance
  - Interrogatories, social media content of third party
PRODUCTION OF SOCIAL MEDIA

- Generally speaking, requesting party is not given access to plaintiff’s social media account
  - Plaintiff simply produces the relevant material requested
  - Some jurisdictions, though, will give unfettered access to social media accounts, e.g., Pennsylvania
  - Occasionally, courts will review social media content in camera or appoint a special master
- Discovery from social media site likely to be unsuccessful (material protected by SCA)
EVIDENTIARY ISSUES

- Relevance
- Authentication (F.R.E. 901)
  - Testimony from person who drafted the posting
  - Comparison method (comparing posting to previously authenticated evidence)
  - Distinctive characteristics, e.g., appearance, content, substance, internal patterns
    - Metadata, hashmarks
EVIDENTIARY ISSUES

- **Hearsay**
  - Computer-generated content is not hearsay because there is no declarant
  - Not offered for the truth of the matter
- **Exclusions**
  - Party admission
- ** Exceptions**
  - Present sense impressions
  - Then-existing state of mind
  - Business records
EVIDENTIARY ISSUES

- **Best Evidence**
  - Print-outs of electronically stored information are treated as originals under Rule 1001
  - But social media evidence is uniquely subject to destruction or loss, so best evidence often an issue
SOCIAL MEDIA CASES

- **State v. Eleck**, 130 Conn. App. 632 (2011) (Facebook message not authenticated because of lack of circumstantial evidence to verify the identity of the person with whom the defendant was messaging)

- **Griffin v. State**, 419 Md. 343 (2011) (admission of MySpace pages was reversible error where proponent advanced no circumstantial evidence of authorship)
SOCIAL MEDIA CASES


- *Ogden v. All State Career School*, 299 F.R.D. 446 (W.D. Pa. 2014) (in sexual harassment case, social media records not relevant under F.R.E. 412 where proposed use was to show plaintiff was not offended, but potentially relevant to show emotional state)
SOCIAL MEDIA CASES

- **Zimmerman v. Weis Markets**, 2011 WL 2065410 (Pa. Com. Pl. 2011) (social media evidence relevant to show that plaintiff, despite claims that health problems diminished his enjoyment of life, was riding motorcycles and stunt bikes)

- **EEOC v. Simply Storage**, 270 F.R.D. 430 (S.D. Ind. 2010) (all content of sexual harassment plaintiff’s social media relevant, even though locked or private, or potentially embarrassing, or invasive of privacy)
SPEAKER CONTACT INFORMATION

- Mark S. Filipini, Partner, K&L Gates LLP
  206.370.8111
  mark.filipini@klgates.com

- Michael A. Pavlick, Partner, K&L Gates LLP
  412.355.6275
  michael.pavlick@klgates.com
QUESTIONS
THANK YOU