K&L GATES

WORK ISSUES IN THE INTERNET AGE

www.klgates.com

Today's Presenters

Michael R. Haven, Esq.
Linda L. Usoz, Esq.

K&L Gates LLP
630 Hansen Way
Palo Alto, CA 94304
(650) 798-6700
mike.haven@klgates.com
linda.usoz@klgates.com

Exclusive Rights to Materials

THE FOLLOWING MATERIALS HAVE BEEN PREPARED BY K&L GATES LLP TO BE USED EXCLUSIVELY BY K&L GATES AND THE ATTENDEES OF THE EMPLOYMENT LAW SEMINAR ENTITLED "WORK ISSUES IN THE INTERNET AGE" AS PRESENTED BY K&L GATES

THESE MATERIALS ARE NOT TO BE REPRODUCED, COPIED, TRANSMITTED OR USED IN ANY MANNER BY ANY PERSON OR ENTITY WITHOUT THE EXPRESS WRITTEN CONSENT OF K&L GATES.

SOCIAL NETWORKING

HOME OFFICE EMPLOYEES

Introduction

- **What is Social Networking?**

  Expanding social and/or business contacts by making connections through individuals.

- **Use of Websites**

  Social networking websites are powerful communications tools. Facebook alone has more than 500 million active users. Other popular sites include LinkedIn, Twitter, and MySpace.

- **Social Networking for Business**

  Social networking sites are increasingly being used by businesses. But to what extent are they appropriate in the workplace, if at all?

  We will analyze the advantages and disadvantages of allowing employees to use social networking sites in the business environment. This will help you develop a social networking policy for your business.

Risk/Benefit Analysis

- There are risks and benefits associated with allowing social networking in the workplace.
- Every business must weigh the risks and benefits and design a policy that meets its particular needs.

Risks of Use

- Decreased Productivity
- Data Protection
- Resources/Bandwidth
- Office Politics
- Liability

Potential for Decreased Productivity

- **Most Common Reason for Blocking Access**
- **The Bottom Line**

  If every employee in a 50 person workforce spent 30 minutes on a social networking site each day, there would be 6,500 hours of lost productivity each year.

- **Company Morale**

  Some employees would be required to pick up slack of abusers. Heightened impact if no action taken by management.

- **Questions to Consider**

  Are social networking websites really to blame for lack of productivity? If blocked would time be wasted on some other form of online activity?

Data Protection

- **Potential for Fraud**

  Hackers target social networking sites because of the potential to launch malware attacks and commit fraud.

  Third party applications (i.e., on Facebook) can infect computers with malicious code and viruses, which in turn can be used to collect user data.

- **Anti-Privacy Phenomenon**

  Voluntary relinquishment of privacy. Users willing to post personal details and data which can be mined by cyber criminals.

  People falling victim to identity theft or online scams that seem genuine.

- **Question to Consider**

  Do social networking sites pose more of a threat than other websites?

Resources/Bandwidth

- **Use of Video**

  Availability of video postings on social networking sites creates problems for businesses due to high levels of bandwidth used and added internet costs.

- **Question to Consider**

  If social networking sites were blocked, would employees still have access to online media?

Office Politics

- **Hypothetical**

  A team of 10 employees is managed by 1 supervisor. The 10 employees have the same job and all work together. The supervisor and 5 of the equal-level employees are friends on Facebook and use the platform to discuss work issues and plot workplace strategies.

- **Questions to Consider**

  How does this affect the 5 employees who are not Facebook friends with their supervisor?

  Should supervisors engage on social networking websites with some members of their team but not others?

Liability

- Privacy Issues
- Harassment
- National Labor Relations Act
- Title VII and Other Discrimination Laws
- First Amendment

Privacy Issues

- California Constitution, Article I, Section 1, states:

  All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy

Common Law Privacy

- Public disclosure of private facts (Duke University student who rated her sexual encounters with Duke athletes; public posting by her friends)

- Intrusion (disclosure of photos, video or other information which are private or where expectation is that they will remain private—peeping tom)

Common Law Privacy (cont.)

- False light (photo of actress and producer with article claiming they were dating where wife of producer was not visible in picture but was present may be false light—*Fellows v. National Enquirer*, 721 P.2d 97 (Cal. 1986))

- Misappropriation of name or likeness (using former professional baseball player's likeness, without consent, to advertise and sell beer is misappropriation—*Newcombe v. Adolph Coors Co., 157 F.3d 686 (9th Cir. 1998))*

Privacy Dependent on Reasonable Expectations

- Employer's policies on information systems

  Employer owns all systems.

  Systems provided to assist employee in performing duties and facilitate company's business.

  Everything that is created, stored, accessed, transmitted, received, manipulated, revised or posted using employer's systems is the employer's property.

Privacy Dependent on Reasonable Expectations (cont.)

- Policy should include right to access, intercept, delete, copy, transmit, store and transfer any information.
- Employer can share information with third parties (including law enforcement) without notice to or consent of employee.
- Use of passwords not affect employer's rights and can be overridden; all passwords must be disclosed to employer.

Implicit Waiver of Privacy

- Items posted by owner of the account; who can access?
- Items posted by “friends” or visitors permitted to post on another’s site
- Ability to email/cut and paste items from someone else’s page to anyone else (including those not otherwise permitted to view the account holder’s web page or site)

Case Study

- ***Pietrylo v. Hillstone Restaurant Group***

  A restaurant employee formed a private, by-invitation-only discussion group on his MySpace page. Intent was to create a forum for his colleagues to vent about their jobs.

  One member of the group provided access to an uninvited manager. Two employees were fired as a result.

  The employees filed claims against the restaurant in federal court, including common law invasion of privacy. The privacy claims survived summary judgment and went to the jury. Jury found no reasonable expectation of privacy.

  The jury awarded damages (including punitive) for violation of the Stored Communications Act.

Unlawful Harassment

Are employers liable for postings on social networking sites which may be unlawfully harassing?

- No case law; will take a few years.
- Employer lacks the ability to control postings on site it does not own or control.
- Employer cannot control off duty conduct or free speech rights outside the workplace.
- But . . . does not mean the employer can ignore entirely.

National Labor Relations Act

- Prohibits employers from disciplining or otherwise retaliating against non-supervisory, non-management employees who engage in “concerted activity” for the purpose of “mutual aid or protection.”

- NLRA applicability to social networking hinges on whether the activity was concerted (i.e., if the employee notified other employees about the social network, discussed aspects of the work environment, and permitted other employees to respond and comment).

- Employers should proceed with caution when multiple employees engage in criticism of the employer on a social network.

Title VII

- **Online Activity Revealing a Protected Characteristic**

  Hypothetical: An employee-blogger who regularly posts about his recent conversion to Islam alleges that his dismissal was a result of his religious beliefs and therefore violated Title VII. He might have a prima facie case for religious discrimination if he can show (1) the employer read his blog, (2) the blog made the employer aware of his religious faith, and (3) subsequent to becoming aware of his faith, the employer fired him.

- **Others Engaging in Same or Similar Activity Not Dismissed**

  In one real (and well known) case, a Delta airlines employee ("Queen of the Sky") was fired for posting on her blog mildly provocative pictures of herself in her Delta uniform. She filed suit alleging that male employees who engaged in similar activity did not face any adverse employment action. (*Simonetti v. Delta*)

Other Discrimination Laws

- Other federal statutes may protect employees from discipline related to online conduct.
- "Whistleblower" or anti-retaliation statutes may protect social networkers who divulge information about their employers on social networks.
- The FMLA protects employees who oppose workplace practices which violate the FMLA. Such opposition could be in the form of a social network post.

First Amendment

- Public employers are limited by the First Amendment when their employees are speaking on matters of public concern.

- Example – City of Redondo Beach

  Redondo Beach had a Facebook page allowing its "fans" to post content on its "wall." Some constituents posted vulgar comments and misinformation. Rather than removing the postings, the City opted to remove its page due to First Amendment concerns.

Benefits of Social Networking Websites

- Despite potential risks, social networking sites are being used safely and effectively for business purposes.
- Can be used *internally* to improve employee communications and collaboration.
- Can be used *externally* to draw on collective community intelligence and seek out and sustain business relationships, leveraging the technology to obtain a competitive advantage.

Benefits of Internal Use

- **Preventing Overloaded Email Inboxes**

  Can replace company email for everyday back and forth communications between employees.

- **Improved Open Communication**

  Allows employees to discuss ideas, post news, and share links. Leads to enhanced information discovery and knowledge.

Benefits of Internal Use (cont.)

- **Productivity Through Collaboration**

  Teams that average more frequent communication among their members can obtain higher productivity.

- **Improved Employee Morale**

  Employees enjoy using social networking sites.

Benefits of External Use

- **Market Research**

  Opportunity to obtain information about the market space. With a good company profile and little cost, new markets and business opportunities become visible.

- **Personal Touch**

  Ability to reach out to groups or individuals and target them personally. Businesses can encourage their customers to become connections or friends, offering exclusive discounts to online contacts.

Benefits of External Use (cont.)

- **Enhance Brand Recognition**

  Ability to boost image as a leader in the field without traditional advertising. Customers/contacts begin to acknowledge your business as reliable and an excellent source of information/products.

- **Low-Cost Marketing**

  Ability to reach out to an increased audience, implement marketing campaigns, announce special offers, make important announcements, and direct interested people to the company's website. Allows consumers to communicate directly with your business. Only cost is time and effort required to maintain the network.

To Allow or Not to Allow

- Should you embrace social networking and accept the risks, or should you block social networking and eliminate the risks?
- Depending on your business model, a hybrid approach may be best. For example, you could allow limited access to those sites which may actually benefit your business while blocking less useful sites.
- How do you devise a policy to accomplish this?

Best Practices for Controlling Use

- Choosing a Filter
- Monitoring Internet Use
- Provisions of a Well-Crafted Acceptable Use Policy ("AUP")
- Off Duty Policies

Choosing a Filter

- Web filters can prevent unauthorized use of the internet, but must be chosen carefully.
- Some filters will operate only to impose a blanket ban on social networking sites for all users.
- Other filters are more customizable and enable businesses to impose user (or group) specific restrictions or block access only at certain times of the day.

Monitoring Internet Use

- Regulations require the creation of an AUP before monitoring the internet use of employees.
- Monitoring can be used (1) to ensure that employees are using company resources in a manner consistent with the AUP, and (2) to shield the business from civil and criminal liability in the case of an employee misusing company resources.
- Monitoring should be automated to take human bias out of the process. Use spot-checking rather than continuous monitoring. Limit monitoring to overall traffic rather than specific items, but target monitoring on high risk areas.

Best Practices for a Well-Crafted AUP

- **General Principles**

  Information posted to social networking sites is in the public domain and could impact the image of your business.

  Educate employees so they know the do's and don'ts of social networking.

  Mostly common sense. **Do** promote the business. **Do** collaborate with colleagues on business matters. **Don't** say negative things about colleagues. **Don't** post inappropriate material.

  Restrictions placed on use (i.e., permissible sites or the times at which they can be visited) must be clearly stated and understood.

Best Practices for a Well-Crafted AUP (cont.)

- **Specifics**

  Must be in writing and clearly describe what uses are permitted (if any).

  If use of social networking sites is permitted, must ensure that such use does not interfere with job duties.

  Must clearly express that employees have no expectation of privacy when using an employer computer system.

Best Practices for a Well-Crafted AUP (cont.)

- **Specifics (cont.)**

  Must express that use of social media cannot violate anti-discrimination policies or other codes of conduct.

  Must prohibit employees from divulging proprietary and/or confidential company information.

  Must prohibit employees from divulging personal information of other employees.

Best Practices for a Well-Crafted AUP (cont.)

- **Specifics (cont.)**

  Must prohibit use of employer logos/brands on personal pages.

  Must express that employees may not state or imply that personal pages represent the company.

  Must include a broad provision prohibiting conduct which violates federal, state, or local law.

Best Practices for a Well-Crafted AUP (cont.)

- **Specifics (cont.)**

  Must include privacy rules for employer and employees.

  Must direct to management all employee questions regarding the AUP.

  Must warn that disciplinary action will be taken if the policy is violated.

Best Practices for a Well-Crafted AUP (cont.)

- **Specifics (cont.)**

  Must explain what monitoring will occur.

  Must be communicated to all employees, contractors, and anyone else who uses the network.

  Provide two copies to each user – one to keep and one to be signed and returned.

Off-Duty Conduct That Affects the Workplace

- Postings mention employees, employer by name.
- Information disclosed on social networking site is discussed in the workplace.
- Issues discussed on social networking sites affect workplace.

Off-Duty Conduct Statutes

- Some states (i.e., California, Colorado, New York) have enacted off-duty conduct statutes which prohibit an employer from disciplining an employee for engaging in lawful conduct while away from the employer's premises.

- Exceptions allow employers to limit otherwise lawful, off-duty conduct where it creates a material conflict of interest for the employer or is reasonably related to the employee's job.

- For example, the New York statute allows an employer to discharge an employee for off-duty conduct that creates a material conflict of interest related to trade secrets, proprietary information, or some other business interest.

Employer Access/Use of Information

- As part of investigation into harassment or other unlawful activities
  - Employer may visit sites to discover publicly viewable postings that may have bearing on investigation BUT
  - Cannot always be certain of identity of person posting the information.
  - Must have connection to workplace (employer is not arbiter generally of appropriate/ inappropriate postings on social networking site).

Employer Access/Use of Information (cont.)

- Items posted without restrictions (i.e., publicly available profile information).
- Items not publicly viewable (i.e., must be a “friend” on Facebook to view certain posted information about a subject).
- Compelled disclosure through court order
  - Stored Communications Act
  - Disclosure can be compelled by court order, even information that has been “removed” or deleted.

UNIQUE WORK ISSUES RELATING TO "HOME OFFICE" EMPLOYEES

Home Office Workers

- Advent of high-speed internet access and “desk top” connectivity to the Employer’s computer systems, along with prevalent use of cell phones and “call forwarding,” have made “working from home” virtually seamless for many ranks of employees that literally would not have been possible just several years ago.

- However, rapid expansion and use of “home office” workers have created unique employment law challenges for many employers.

- A sampling of these issues are explored below.

Definitions of Home Office and Home Worksite

- The U.S. Department of Labor, in February 2000, issued an OSHA "Instruction" to all OSHA personnel in connection with OSHA enforcement, and defined "home-based worksite" and "home office" as follows:
  - **Home-Based Worksite**: The areas of an employee's personal residence where the employee performs work of the employer.
  - **Home Office**: Office work activities in a home-based worksite (e.g., filing, keyboarding, computer research, reading, writing). Such activities may include the use of office equipment (e.g., telephone, facsimile machine, computer, scanner, copy machine, desk, file cabinet).

OSHA and Home Office Employees

- OSHA applies to any private employer who has any employees doing work in a workplace in the United States. It requires these employers to provide employment and a place of employment that are free from recognized, serious hazards, and to comply with OSHA standards and regulations.
- In 1999, the Department of Labor (DOL) issued an "Instruction" or guidance under OSHA that would have required Employers to inspect the "home office" of its employees to ensure safety, and this caused a major controversy and uproar.
- As a result, that position was withdrawn and replaced.

OSHA and Home Office Employees (cont.)

- Instead, the 2/25/2000 Instruction was issued by the DOL which provided in relevant part as follows:
  - OSHA respects the privacy of the home and has never conducted inspections of home offices.
  - OSHA will not conduct inspections of employees' home offices.
  - OSHA will not hold employers liable for employees' home offices, and does not expect employers to inspect the home offices of their employees.

- However, Employers are responsible in home worksites for hazards caused by materials, equipment, or work processes which the employer provides or requires to be used in an employee's home.

Reporting of Accidents by Home Office Workers

- Employers who are required, because of their size or industry classification, to keep records of work-related injuries and illnesses under OSHA, will continue to be responsible for keeping such records, regardless of whether the injuries occur in the factory, in a home office, or elsewhere, as long as they are work-related, and meet the record keeping criteria. (2/2000 Instruction)
- Similarly, Employers should report work-related injuries suffered by home office workers to their Workers' Compensation insurance carriers.
- Employers should have special policies in place to ensure that home office workers promptly report injuries.

FMLA/CFRA Leave Issues

- Under the FMLA and California CFRA, in order to be eligible for protected leave, the employee must (in addition to other factors) work for an Employer who employs 50 or more employees within 75 miles of the worksite where the employee is employed.
  - If the home office is within 75 miles of a Company office or facilities that has 50 or more employees, then this condition is satisfied
- At first blush, it would appear that if the employee was working at a remote home location, then the employee would not be covered. **However, the employee may be covered due to a special Regulation.**

FMLA/CFRA Leave Issues (cont.)

- FMLA Regulation 29 CFR § 825.111(a)(2) states in relevant part as follows:
  - **An employee's personal residence is not a worksite in the case of employees**, **such as** salespersons, who travel a sales territory and who generally leave to work and return from work to their personal residence, or **employees who work at home**, as under the concept of flexiplace or telecommuting. Rather, **their worksite is the office to which they report and from which assignments are made.** (Emphasis added.)

FMLA/CFRA Leave Issues (cont.)

- Federal cases interpreting this Regulation have concluded that if the employee regularly reports and receives assignments from an office that has 50 or more employees within 75 miles, then the home office employee will be deemed covered for FMLA purposes, even if the home office employee is not located within 75 miles of any other employees.
- California CFRA will generally incorporate FMLA Regulations in applying the CFRA, unless the Regulation conflicts with a specific provision of the CFRA (which does not appear to be the case here.) Accordingly, although no California case has addressed this issue, it appears that CFRA coverage will also apply.

FMLA/CFRA Leave Issues (cont.)

- Questions have arisen as to whether a home office employee who reports to another home office employee (who in turn reports to a covered facility) would be covered under the FMLA or not, but the cases are split on authority on this issue. (See, for example, *Killion v. Hospira Worldwide, Inc.,* 2009 U.S. Dist. LEXIS 7492)

- Employers with large numbers of home office workers who are spread out over expansive territories may wish to consider establishing a small satellite office for all of those employees to report (rather than reporting to another employee's home office or to the main office with 50 or more employees) in order to avoid potential FMLA and CFRA coverage issues.

Timekeeping for Non-Exempt Employees

- "Non-exempt" home office workers are still covered by wage and hour laws.
- Employer has obligation to keep track of hours worked.
- Meal periods still need to be "provided" and recorded.
- Implement accurate methods for recording time.
  - Rather than arriving at set time and leaving at end of day, home office workers may tend to work in blocks of time spread out over longer hours or night.
  - All time worked from home needs to be accurately reported as worked on the actual day/time on which it was worked.
- May want to provide special training on time recording to avoid potential "off the clock" and overtime claims.

Supervision of Non-Exempt Employees

- Employer loses ability to directly supervise and monitor employee performance.
- Employers instead need to monitor output and work product based on objective performance standards to ensure that “work” is being performed.
- Some job positions may require regular ongoing communications with company via email or phone anyway.
- Other positions, however, may require some “reporting” on a regular interval basis to ensure employee “is still there.”

Employee Privacy Concerns

- Employees are protected by a "right to privacy," even at Employer's workplace. (Cal. Const., Art. I, Sec. 1)
- Involves a "balancing" between the Employer's legitimate business interests and the employee's expectations of privacy.
- Home office employees will have even greater expectation of privacy in their home.
  - While Employer may have right to inspect employee desk at company office at any time, likely not going to happen at home office.
- May want to consider written agreement allowing certain limited access to home office to inspect.

Protecting Confidential Information

- If employee works with confidential information, may require special safeguards to protect at home office.
- Identify in written agreement special procedures by employee to keep info confidential at home office.
  - Limitations on who has access to computer.
  - Proper security, anti-virus and encryption installed.
  - Special methods for storing confidential documents at home (under lock and key).
  - Obligation to immediately notify Employer if security is ever breached.
  - Grant to Company limited access to obtain/retrieve.

Protecting Company Equipment at Home Office

- Certain work may require special equipment to be installed at home office.
  - Special computers, printers, faxes or machines.

- If so, then also recommend written agreement identifying special procedures to safeguard at home.
  - Limitations on who has access to equipment.
  - Special methods for storing at home and keeping under lock and key when not in use.
  - Obligation to immediately notify Employer if stolen.
  - Agreement not to use for personal use.
  - Grant Company limited access to obtain/retrieve.

Use of Employee Equipment at Home Office

- California Labor Code § 2802 provides that an Employer shall indemnify the employee "for all necessary expenditures…incurred by the employee in direct consequence of the discharge of his or her duties…"
- Labor Code § 2804 provides that "any contract or agreement, express or implied, made by any employee to waive the benefits of [§ 2802] is null and void…"
- The California Supreme Court has held the benefits of § 2802 cannot be waived by agreement or release. (*Edwards v. Arthur Andersen*, 44 Cal. 4th 937 (2008))
- Accordingly, the Employer will have an obligation to reimburse the employee for costs incurred at home.

Use of Employee Equipment (cont.)

- The Employer may require the employee to have certain equipment as a condition of employment without having to purchase that equipment.
  - Required use of personal car for work does not obligate employer to purchase the vehicle, but the Employer will be required to pay for the cost of the **use** of that vehicle (usually by reimbursing the employee at the approved IRS mileage rate).
- No case on point, but Employer could probably require the employee to have personal computer as a condition of working from home office if employee has choice of working at Company office or from home.

Use of Employee Equipment (cont.)

- Cases interpreting Labor Code § 2802 usually require Employer to reimburse employee for "reasonable and necessary" expenses incurred by employee in performing their job.
- May require Employer to reimburse employee for monthly cost of high-speed internet access, or at least that proportion that is used for work-related use.
- May also require employee to reimburse employee for printing paper, ink, and related printing supplies.
- Reimbursement for cost of telephone charges from home, either for direct calls or portion of monthly service charges, also likely required by § 2802.

Use of Employee Equipment (cont.)

- Although the Company may have standard business expense reimbursement policies, it is recommended that a special policy or written agreement for home office workers should be used to clearly spell out those regularly recurring monthly expenses and costs that will be reimbursed by the Employer to avoid "surprises" in the future.
- Additionally, although the protections of § 2802 cannot be waived, the parties should be able to voluntarily agree as to whether certain costs will be deemed legitimate business expenses, and having the written agreement may help establish that other expenses were not reasonable and necessary.

Use of Employee's Home Telephone Line

- Additional issues and concerns are raised where employee is using a personal phone line for work use.
  - Steps to ensure that phone line will be clear and not used by family members.
  - Proper procedures for answering calls.
  - Same for cell phone use.

- Bigger concern may be Company access or ability to obtain the phone number used if phone line is in employee's name following termination of employment.
  - Better method is for Company to install business line in Company name and pay for monthly bills, so that Company can control the phone number.

"Posting" Requirements at Home Office Sites

- Many laws and regulations require Employers to "post" various notices in the workplace, such as EEOC, DFEH, Sexual Harassment, Wage and Hour, OSHA, Workers' Compensation and many others.
- Selected review of these Regulations indicates that they do not specifically address Home Office workers.
- Informal discussions with various government agencies indicate that they do not believe Employers are required to "post" notice at employees' homes.
- However, it is recommended that such employees be mailed copies of all such notices, especially key notices such as EEOC/DFEH and sexual harassment postings, Wage Orders, and Workers' Comp.

Other Potential Home Office Issues

- To reduce likelihood of discrimination claims, Employers should use clearly defined, objective standards to grant or deny employee requests to telework, and should consider centrally administering such requests.
- Allowing employees to telework could impact what reasonable accommodations the Employer must provide to future disabled employees requesting accommodation (i.e., it may be harder for Employer to argue that telework creates an undue hardship). In addition, Employer may be obligated to provide home-based accommodations for teleworking employees (special office equipment in home office, etc.) in some situations.

Other Potential Home Office Issues (cont.)

- If employees are allowed to work from a home office in a state other than California, additional or different state employment laws/taxes may apply. Employer should require employees requesting telework to disclose the city and state where they would be working in order to assess potential legal issues.

Home Office Worker Recommendations

- Often good practice for Employer to enter into written agreement with each home office worker that addresses a variety of employment issues, such as:
  - Ability of employer to inspect employee's home office
  - Duty of employee to promptly report accidents in home office
  - Duty of employee to take specific steps to keep work documents and data confidential
  - Duty of employee to enter all time worked from home accurately and per company procedures, etc.

QUESTIONS and ANSWERS