CYBERSPACE AND BEYOND: HANDLING ELECTRONIC COMMUNICATIONS AND MEDIA ISSUES

A Webinar Panel Presentation by

***EPIC** – Employment Practices Improvement Committee*

The presentation will start at **10:00 a.m.**

- Please dial 1-866-740-1260
- access code: 987-9289 for audio portion of this program
- PLEASE MUTE YOUR PHONE
- PLEASE DO NOT PUT US ON HOLD

Cyberspace and Beyond: Handling Electronic Communications and Media Issues

A Panel Presentation sponsored by ***EPIC*** – UC's Employment Practices Improvement Committee

PANELISTS

- **Will Carroll –** Schiff, Hardin LLP
- **Stephen Lau –** Director, Systemwide Information Technology Management & Policy, UCOP
- **Greta Schnetzler –** Deputy Counsel, UCSF
- **Pamela Thomason –** Title IX Officer, Sexual Harassment Coordinator, UCLA
- **Moderator: Valerie Shelton–** Senior Counsel, Office of the General Counsel, UCOP

OVERVIEW

- What are the points where employment laws, electronic media and University policy meet?
  - This presentation will help you navigate that intersection by:
    - Reviewing applicable law and policy
    - Providing practical examples of situations where they may need to be applied
    - Anticipating new issues that are arising in the realm of social media

ELECTRONIC COMMUNICATIONS POLICY (ECP)

- Significant difference in privacy in an academic vs. traditional corporate environment
- The ECP views privacy similarly to other academic institutions
- A systemwide policy, applies to all Campuses equally
- Applies to all members of UC, e.g. students, faculty and staff

ELECTRONIC COMMUNICATIONS POLICY (CONT'D)

- Key areas that it covers:
  - Privacy and Confidentiality (Access with/without Consent)
  - Acceptable / Unacceptable Uses
  - Incidental Personal Use
    - http://www.ucop.edu/ucophome/policies/ec/

PRIVACY AND CONFIDENTIALITY

- Prohibits monitoring of "electronic communications" without consent, except:
  - when required by and consistent with law
  - when there is substantiated reason to believe that violations of law or of University policies
  - when there are compelling circumstances, e.g. bodily harm, property loss, evidence destruction
  - under time-dependent, critical operational circumstances

PRIVACY AND CONFIDENTIALITY (CONT'D)

- Obtaining access
  - Each campus has an Access w/o Consent Process and an ECP Coordinator
    - ECP Coordinators
    - http://www.ucop.edu/irc/policy/ecp/coords.html
    - Sample Processes
      - San Francisco
      - http://its.ucsf.edu/EIS/policies_guidelines/AccessWithoutConsent.html
      - Los Angeles: http://www.adminpolicies.ucla.edu/pdf/410.pdf

PROHIBITED USES

- unlawful activities
- commercial purposes not under the auspices of the University
- personal financial gain
- personal use inconsistent with Incidental Personal Use
- uses that violate other University or campus policies or guidelines

INCIDENTAL PERSONAL USE

- Realistically acknowledges that UC members conduct personal activities on UC Resources

- Incidental use must not:
  - Interfere with the University's operation of electronic communications resources;
  - Interfere with the user's employment or other obligations to the University;
  - Burden the University with noticeable incremental costs.
    - Broad and permissive

Note: Limitations under the Public Records Act and Information Practices Act.

PRIVACY RIGHTS ARISE FROM DIFFERENT SOURCES

- U.S. Constitution- Fourth Amendment Prohibition Against Unreasonable Search and Seizure
- California Constitution.- Article I , Sec. I
- Tort Law
- Statutory Restrictions On Access To Private Information
- Contractual Restriction
- California Information Practices Act

GOVERNMENT EMPLOYER'S REVIEW OF TEXT MESSAGES SENT BY EMPLOYEE

- Does employee have reasonable expectation of privacy in texts?
- If so, is employer's search for a legitimate purpose?
- If so, is search reasonably related to that purpose, and not unduly intrusive?
- *Quon v. Arch Wireless Operating Co, Inc.*: U.S. Supreme Court upheld legality of City's search of text messages sent via employer-issued pager, under the facts presented.

NLRB CONSIDERS SOME SOCIAL MEDIA POLICIES TO VIOLATE LABOR LAWS

- Two separate NLRB offices have indicated their position regarding internet policies that seek to prevent employees from criticizing their employers or bosses publicly in social media
- Such policies may violate labor laws that protect concerted action of employees in discussing or criticizing terms and conditions of employment

PRIVACY RIGHTS ARISING UNDER TORT LAW

- Four different types of tort claims recognized in California:
  - Intrusion into private matters ("invasion of privacy");
  - Public disclosure of private facts;
  - Publicity placing a person in a false light;
  - Misappropriation of a person's name or likeness.

INVASION OF PRIVACY

- This tort has two elements:
  - (1) intentional intrusion into a private place, conversation or matter, including private affairs or concerns; (2) in a manner highly offensive to a reasonable person.
  - Generally, plaintiff prove he or she had a ***reasonable expectation of privacy*** in a matter which was ***unreasonably intruded upon*** by the defendant.

STATUTORY RESTRICTIONS ON ACCESS TO PRIVATE INFORMATION

- Arrests not resulting in conviction
- Polygraph exams
- Consumer credit reports
- Investigative consumer reports
- Medical information.
  - HIPAA
  - ADA
  - Confidentiality of Medical Information Act
  - Workers' Compensation

STATUTORY RESTRICTIONS ON ACCESS TO PRIVATE INFORMATION (CONT'D)

- Social Security numbers.
- Identity theft protection.
- California Penal Code prohibitions against electronic eavesdropping or recording.
- Federal Electronic Communications Privacy Act (Wiretap Act)
- Stored Communications Act (SCA)
- FERPA, IPA
- Duty to protect personal information (Civ. Code Sec. 1798.81.5

A CAVEAT….

- Some information about University employees may be considered public and subject to disclosure upon request under the California Public Records Act
  - Salary and incentive information
  - Emails about University business
  - Phone records pertaining to University business
  - Professional calendar information

USING SOCIAL NETWORK SITES TO SCREEN CANDIDATES

Human resources professionals and managers are increasingly using social networking sites, such as MySpace, Facebook, and LinkedIn, to gather information about applicants.

Do the risks outweigh the benefits?

USING SOCIAL NETWORK SITES TO SCREEN CANDIDATES (CONT'D)

- Survey participants identified a range of web-based information which played a role in rejecting candidates, including: bad-mouthing previous employers or fellow employees; publishing information about drinking or drug use; sharing confidential information from previous employers; and publishing provocative or inappropriate photographs.
- "Privacy" restrictions on social networking sites do not eliminate access to such information.
  - Restrictions are optional, and are used by a minority of participants.
  - Information can be re-published by authorized users in unrestricted venues.

LET THE SCREENER BEWARE

Lack of reliability of online information – positive or negative.

- Individuals may manipulate – or fabricate – information to create a positive (or falsely negative) web-profile.

- Websites such as DefendMyName.com and Internet-Reputation-Management.com furnish services and strategies for scrubbing or even enhancing online "reputations."

TOO MUCH INFORMATION?

- Various statutes restrict information employers may inquire into or consider in making hiring decisions. For example:

  - Employment discrimination laws prohibit consideration of a range of characteristics about an applicant, including the applicant's race, religion, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, age or sexual orientation (Govt Code Section 12940(a).

TOO MUCH INFORMATION? (CONT'D)

- Employers cannot ask job applicants questions regarding any arrest or detention that has not resulted in conviction of a crime or participation in a diversion program. (There are limited exceptions for certain minor marijuana-related offenses, and for arrests for which the individual has been released on bail or is on his or her own recognizance.) (Cal. Labor Code section 432.7(a)).

TOO MUCH INFORMATION? (CONT'D)

- California's Investigative Consumer Reporting Agencies Act ("ICRAA") applies to third-party employment screeners as well as employers who conduct their own background checks. The ICRAA prohibits reporting pertaining to a variety of matters, including conviction of a crime that, from the date of disposition, release or parole, is more than seven years old; bankruptcies more than 10 years old; lawsuits and judgments more than 7 years old; and other adverse items of information that antedates the report by more than 7 years. (Cal. Civil Code section 1785.13(a)(7)).

LIMITING THE ROLE OF ONLINE BACKGROUND CHECKS

- While employers know to avoid inquiring into protected categories during the formal application process, such information about an applicant is routinely available on the web.

- Employers who encounter (or gather) such information about an applicant who is subsequently rejected may have to prove that the information played no role in the hiring decision.
  - Any online searching should be done by an employee who does not play any role in the hiring decision. Any input into the hiring process by this person should be limited to a report which solely addresses objective information that may lawfully be considered as part of the hiring process.

FIRST AMENDMENT AND ACADEMIC FREEDOM

- APM 101:
  - "The principles of academic freedom protect freedom of inquiry and research, freedom of teaching, and freedom of expression and publication."
  - "The exercise of academic freedom entails correlative duties of professional care when teaching, conducting research, or otherwise acting as a member of the faculty. These duties are set forth in the Faculty Code of Conduct (APM-015)

Generally, speech by professors in the classroom is protected under the First Amendment if the speech is "germane to the subject matter." Also, such speech in academic journals or conferences is protected. What about academic speech online?

USE OF ELECTRONIC MEDIA IN INTERNAL INVESTIGATIONS

CELL PHONES

- Date, time, length of call
- Frequency
- Text messages
- Location

SOCIAL MEDIA SITES

- Photos
- Postings
- Messages
- AOL screen name
- Friend lists

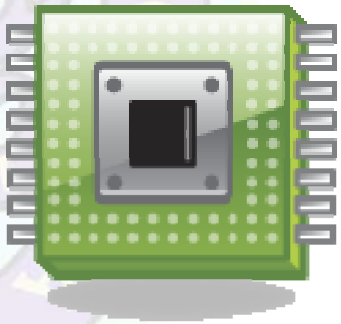
BLOGGING

- Like Facebook, a blog can provide a lot of background information about a person.

- Sometimes the blog itself is offered as evidence of harassment.

USE OF ELECTRONIC MEDIA TO ENGAGE IN UNLAWFUL ACTIVITY

- Sexual harassment
- Gossip
- Stalking



HYPOTHETICALS

INTERNET SHOPPING AT WORK

A Supervisor sees that employee is surfing the net, price shopping for personal goods, instead of working.

- Can Supervisor counsel him on internet use? Can he restrict him from internet use? What are scope of restrictions?
- What if the supervisor knows that the employee is a poor performer and, in particular, does not complete assignments in a timely manner? Can he monitor the employee's internet use?
- What if the supervisor knows that the employee is frequently on the internet for personal use and observes him internet shopping or using his personal email account to send messages? Can he then ask to monitor the employee's internet use? Does he need to tell the employee first?

PARIS HILTON REVEALED

- From time to time, emails are sent from an administrative assistant with non-identified attachments to her professor. The latest attachment showed Paris Hilton in her famous sex video. Unknowingly, the professor opens the attachment while his office assistant is present. She does not complain but it becomes widely known in the department that the professor views pornography.

- What action, if any, should be taken?

OFFENSIVE WEBSITE BY UC EMPLOYEES

- Several lab employees have developed a website that features a picture of the lab superimposed with labels such as “Girls Gone Wild” and “Get Your Strippers Here”. The lab is clearly identifiable as a UC lab.

- Can any action be taken against the employees who posted the site?
- What if a co-worker views the site at home and reports being offended?

BLOGGERS BEWARE

- An employee starts a blog that criticizes University administration of mismanagement, naming individuals and calling them incompetent and greedy and referenced as “crooks, whores and politicians”. Others are invited to join in with specific stories from their particular campus/work location and several do, without identifying themselves.

- What if another employee is witnessed responding to the blog while at work?

MAD MARIE

- Mad Marie is an emergency medical tech who is questioned by her supervisor about a customer complaint regarding her work. Marie is upset by the questions asked of her. As a result, she posts negative comments on her Facebook account from her home computer, writing that she "loved how the company allows a psychiatric patient to be a supervisor. Co-workers responded sympathetically. She then responds to the comments by referring to her supervisor as, among other derogatory terms, a "scumbag".

- Can she be terminated for posting defamatory, discriminatory or disparaging comments about her supervisor?

THE SWEATY SISTERS GOSSIP SITE

- Suzie is an advisor in fraternity and sorority relations within student affairs. Following a drug and alcohol prevention presentation to one fraternity, she receives an anonymous email joking about the presentation and sending her a link to a web site known as “Sweaty Sisters.” The Sweaty Sisters site is a gossip site on which students may make anonymous postings. The site includes remarks disparaging the chancellor’s conservative wardrobe and claiming, with considerable explicit detail, that he engages in public sex acts.

- Can anything be done about either the website or the comments about the Chancellor?

THE MOLE

- A professor who uses animals in her research noticed a new lab assistant looking at a website denouncing the "torture" of animals by research scientists. Concerned that the employee may be a "mole" for animal rights activists, she accesses the assistant's computer after hours. In a folder labeled "stuff" stored on the computer's hard drive, the professor finds what appear to be draft blog postings accusing her lab of inhumane treatment of animals. The postings are signed "rat@ucberkeleylab." The professor does a web search, and finds numerous postings from "rat@ucberkelylab" on a website that is infamous for publicizing home demonstrations aimed at UC researchers, some of which have resulted in vandalism and threats. The professor insists that the assistant be fired immediately.

- Should the employee be fired?

FACEBOOK FRIENDS

- An academic department is seeking to fill a senior administrative position. Fred, one of the individuals on the hiring committee "Googles" one of the leading candidates, Sally, and pulls up her Facebook page. The page's privacy setting lists certain "friends" of Sally, but restricts access to her profile, pictures, etc. Fred knows one of Sally's "friends" listed on the page. He asks that person to show him Sally's page. In reviewing the page, Fred notes various pictures of Sally at several parties in various stages of apparent intoxication. In one photo, a reveler appears to be passing a joint to Sally. He describes his findings to the Committee at its next meeting, and criticizes Sally for her "immature" behavior. The Committee selects another candidate for the job.

- Were the committee's actions proper?

DEAN CHEEERS

- Associate Dean Cheers is frequently observed by his staff to be online on websites that involve buying and selling of rare wines on the Asian market. An anonymous whistleblower complaint is filed alleging that Associate Dean Cheers is misusing University time and resources to operate a for-profit business of trading in rare wines for profit.

- Can the University check his web use to determine whether this is the case? If so, how would that be done?

- Cheers' response is that this is a hobby only and he has never made money from this activity. How might the investigatory go about proving or disproving that "defense?"

Thank you