April 2015

Electronic Privacy in Higher Education (CLE)

Ray Haines
The State University of New York

Frederick Lane

Jill L. Rosenberg
Herrington & Sutcliffe LLP

Jason Walta
National Education Association

Follow this and additional works at: http://thekeep.eiu.edu/jcba

Part of the Collective Bargaining Commons, and the Higher Education Commons

Recommended Citation
Haines, Ray; Lane, Frederick; Rosenberg, Jill L.; and Walta, Jason (2015) "Electronic Privacy in Higher Education (CLE)," Journal of Collective Bargaining in the Academy: Vol. 0 , Article 31.
Available at: http://thekeep.eiu.edu/jcba/vol0/iss10/31

This Proceedings Material is brought to you for free and open access by The Keep. It has been accepted for inclusion in Journal of Collective Bargaining in the Academy by an authorized editor of The Keep. For more information, please contact tabruns@eiu.edu.
NATIONAL CENTER FOR THE STUDY OF COLLECTIVE
BARGAINING IN HIGHER EDUCATION AND THE
PROFESSIONS—42ND Annual National Conference

April 20, 2015

Electronic Privacy in Higher Education: Balancing The
Interests of Employees and Employers

Ray Haines, The State University of New York
Frederick Lane, Author and Attorney
Jill L. Rosenberg, Orrick, Herrington & Sutcliffe LLP
Jason Walta, National Education Association
Ubiquity of Employer Monitoring

- 43% monitor workplace email, mainly through computer software (73%)
- 66% track web activity at work
- 43% store and review computer files
- 45% track key stroke activity
- 12% monitor blogs
- 10% track social media sites

Sources: 2010 Ponemon Institute Workplace Privacy Study; 2009 survey by AMA and E-policy institute
Consequences Often Dire

- 28% have fired for employee misuse
  - Violations of policy (64%)
  - Inappropriate material (62%)
  - Excessive use (26%)
  - Breach of confidentiality (22%)

- 30% have fired for internet misuse
  - Violations of policy (48%)
  - Inappropriate viewing or downloads (84%)
  - Excessive use (34%)
But Training Often Lacking

- 80% of employers have written electronic communications policies
- Less than 50% train on internet risks, policies and usage
Accessing Employee Data: Legal Framework

• Constitutional Law
  – Fourth Amendment
  – State Constitutions

• Federal Statutory Law
  – Electronic Communication Protection Act (ECPA) (18 U.S.C. 2510 et seq.)
  – Common Law
Accessing Employee Data: Legal Framework

• ECPA/SCA
• Title I: prohibits interception of electronic communications
  • Interception must be during transmission
  • Obtaining stored communications is not an interception
• Title II: prohibits “unauthorized access” of stored electronic communications
Workplace Technology Policies

- Have an acceptable usage policy
- Institution’s ownership of IT Resources and electronic documents contained therein
- Institution’s reservation of right to access and monitor without prior notice to the extent permitted by law
- Specify the types of communications and activities that may be monitored (e.g., incoming and outgoing e-mails, documents, social media posts, internet usage)
Workplace Technology Policies

- Specify potential methods of monitoring (e.g., recording, capturing keystrokes, network sniffing technologies). Prohibit all personal use?
- Allow limited personal use at risk of being monitored
- Train managers regarding the policy so they don’t abrogate it with their own statements
Most Employers Search Applicants Online

- >50% formal hiring requirement
- 70% have rejected applicant
  - Search engines like Google 78%
  - Social networking sites  68%
  - Photo and video sharing sites  59%
  - Business networking sites  57%
  - None     2%

Source: Cross-Tab Marketing Research; 2010 Microsoft survey
Pre-Hire Online Checks

- Asking candidates to provide access/passwords
- Problem of too much information
  - Discrimination
  - Activities protected by NLRA
  - State legal activities laws
  - First Amendment for public employees
- Negligence – searching wrong person
- Using third parties to conduct searches – Fair Credit Reporting Act (FCRA)
Best Practices for Employers

- Policy and protocol controlling access to social media sites
- Keep decision makers out of the process
- Train managers and human resources staff
- Conduct search after interview or make contingent offer
- Only search for job related information
- Only search public sites
- Get employee authorization; consider third party vendor
- Maintain records of searches performed and results obtained
Using Monitoring to Support Discipline or Discharge

- NLRA issues/Section 7 rights
  - Overly broad social media policies
  - Retaliation for protected activity
- First Amendment rights
- Off duty conduct
  - State legal activities laws
  - Just cause
Overly Broad Social Media Policies

- No discussion of wages, working conditions, personnel matters
- No disrespectful or disparaging remarks about institution or employees
- No institution affiliation on social media
- No discussion of “internal policies”
- No depiction of institution or logo without consent?
Social Media Policies: Best Practices

- Link policy back to basic values and requirements found in Code of Conduct and existing institution policies
- Eliminate language that may be overbroad, e.g., prohibitions on postings that “may cause damage to the institution’s reputation”
- Provide specific examples of conduct that is prohibited so that employees (or the NLRB) will not erroneously conclude that the policy prohibits Section 7 activity
- Train HR to contact the Legal department before administering any discipline related to employee use of social media
Scope of Discovery of Electronic Media in Litigation

- Determining relevance
- Access to private information
- Use of in camera review
Methods of Discovering Electronic Media

- Pre-litigation public access
- Requests to parties/users
- Requests to third-party providers – SCA
- Tools to access Facebook materials
Labor Laws and Electronic Privacy

Private sector: National Labor Relations Act
  – Threshold issues for higher ed
    – “Employee” status? Yeshiva / Pacific Lutheran
    – “Employer” status? Catholic Bishops / Pac. Lutheran

Public sector: State collective-bargaining laws
  – Often modeled on NLRA
National Labor Relations Act

- Section 7: Right to engage in union activity and “other concerted activities for the purpose of . . . mutual aid or protection.”

- Section 8(a)(5): Unionized employer must bargain before making changes to terms and conditions of employment.
NLRA Section 7

- Protects right to criticize and comment on working conditions online. *Hispanics United of Buffalo* (2012).

- Provides limited right to use employer email system to discuss working conditions and union activity. *Purple Communications* (2014).

- Prevents employers from having overly broad computer use and social media policies that arguably inhibit discussion of working conditions. *Three D, LLC* (2014).
NLRA Section 8(a)(5)

- Employer may not conduct hidden video surveillance of employees without notifying the union and bargaining. *National Steel* (7th Cir. 2005); *Brewers & Maltsters* (D.C. Cir. 2004).

- Employer may not change e-mail and computer use policies without notifying the union and bargaining. *Associated Servs. for the Blind* (1990); *California Newspapers Partnership* (2007)
State collective bargaining laws: Protected/concerted activity

- Protects right to criticize and comment on working conditions online. *New York Division of Parole* (2008).

- Provides limited right to use employer email system to discuss working conditions and union activity. *Fla. Bd. of Educ.* (2003).

- Prevents employers from having overly broad computer use and social media policies that arguably inhibit discussion of working conditions. *Orange County (Fla.) Bd. of County Commissioners* (2011).
State collective bargaining laws: Duty to bargain


- Changes to employer’s computer use policy required notice and bargaining. Vermont State Employees' Ass’n (2009)

- But…not true everywhere. Kansas State Troopers Ass’n (1990) (electronic surveillance is not a mandatory subject of bargaining because it is already regulated by criminal and civil statutes, as well by the Fourth Amendment of the U.S. Constitution)
“Just cause” under CBAs and civil service laws

- Off-duty vs. on-duty conduct
- Clarity of employer rule
- Degree of fault
- Prior service/performance
- Damage to employer
“Just cause” under CBAs and civil service laws

*Land* (Mich.) (2010): No “just cause” to terminate teacher after photographs were posted on a website showing her engaged in oral sex with a male mannequin during an off-duty party.

*Warren County Bd. of Educ.* (Ohio) (2007). “Just cause” supported termination of a teacher’ whose estranged wife posted obscene nude photographs of him on websites and on social media page (so-called “revenge pornography”).
Surveillance of Employees

• Who Are You?
• Where Are You?
• What Are You Doing?
• When Were You Doing It?
• Why Were You Doing It?
• Selfie-Preservation
Who Are You?

- **Purposes**
  - Identity, Security

- **Tools**
  - ID Badges / Smart Badges
  - Prints: Finger / Palm / Voice
  - The Eyes Have It (Retina / Iris)
  - Facial Recognition
  - Typing Pattern / Gait / Ears / Smell, etc.
Where Are You?

- **Purposes**
  - Efficiency, Access Control, Liability

- **Tools**
  - Computer Logins
  - Card Swipes
  - Badge Readers (Infrared / RFID / iBeacon)
  - Vehicular and Mobile GPS
  - Credit Cards
  - Social Media Monitoring and Analysis
What Are You Doing?

• **Purposes**
  – Productivity, Efficiency, Liability, Insurance

• **Tools**
  – Electronic Monitoring (Computers/ Networks)
  – Video Surveillance
  – Sociometric Badges, Cellphones
  – Credit Cards
  – Social Media Monitoring and Analysis
When Were You Doing It?

- **Purposes**
  - Productivity, Efficiency, Liability

- **Tools – Anything With A Time Stamp**
  - Electronic Monitoring (Computers/ Networks)
  - Video Surveillance
  - Credit Cards, EZ Pass, etc.
  - Social Media Monitoring and Analysis
Why Were You Doing It?

• **purposes**
  - Liability, Criminal Investigations

• **Tools**
  - Intensive Digital Investigations
  - Data Mining of Social Media
  - Computer Forensics of Business and Personal Electronic Devices
Selfie-Preservation

• Understand How Technology Works
• Choose Your Employer Carefully
• Understand Your Employer’s Policies
• Keep Business and Personal Data Separate As Much As Possible
• Think Before Posting!
• There Is No Privacy on An Employer’s Network
• Advocate for Openness and Least Invasive Policies
BYOD Privacy Issues

- CFAA and SCA
- HIPAA/GINA
- FCRA
- State laws
- International Laws
Considerations for Employers Re BYOD Policies

- Define the Scope
- Define Appropriate Use
- Define Cost and Support Issues
- Implement Security Protocols
- Consequences for Violations
- Monitoring Access
- Monitoring Use
- Training
Considerations for Employees/Unions Re BYOD Policies

- 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
- Employees: read the policy!
- Back up all personal files, photos, music
GPS Tracking

• “Trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-hotel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on. What the technology yields with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy reference, of our associations – political, religious, amicable and amorous… – and the pattern of our professional and avocational pursuits.”