VENABLE® LLP

“Big Brother” in the Office: Helping Nonprofits Manage Employee Privacy in the Modern Workplace

March 21, 2012
12:30 – 2:00 pm EDT

Moderator:
Jeffrey S. Tenenbaum

Panelists:
David Warner
Grace Lee

VENABLE® LLP

Overview

- Why are we concerned?
  - Technology trends
  - Workforce realities
  - Increasing challenges
- Legal landscape
  - Monitoring generally
  - Work v. Personal device
- Social media
- Policies and practical tips
- Background checks

VENABLE® LLP

Technology

- Increased ability for employers to monitor employee computers and e-mail
- Texting, e-mail, BlackBerries, iPhones, iPads, tablets, etc. allow employees ability to work anywhere anytime
- Work equipment being used for personal matters
- Personal equipment being used for work matters
- Increased use of social media, blogs, for both personal and work matters
- Blurred lines between work and personal life

VENABLE LLP

Technology

- 2009 Survey by ePolicy Institute and American Management Association found that
  - 79 percent of employees had used e-mail to send or receive personal messages
  - 83 percent of employers have rules and policies in place restricting personal use of company equipment
  - 28 percent of employers have fired workers for e-mail misuse, and of those, 26 percent said it was for “excessive personal use”
  - Of companies that monitor e-mail, 73 percent use technology tools to automatically monitor e-mail, and 40 percent manually read and review e-mails

VENABLE LLP

Legal Landscape

- Electronic Communications Privacy Act
  - Covers all forms of digital communications, including private email
  - Generally prohibits
    - Unauthorized and intentional interception of wire, oral, and electronic communications during the transmission phase, and
    - Unauthorized accessing of electronically stored wire or electronic communications
  - Employers are largely exempt from ECPA under one of two exceptions
    - If employer is the provider of the e-mail, Internet, network service, or
    - Employer has implied or express consent of the employee (i.e., employee has knowledge of the employer's policy and continues to use the system anyway, or employee signs acknowledgement of employer's policy regarding privacy and monitoring)
- Fourth Amendment
  - Applies to government employees

VENABLE® LLP

Legal Landscape

- State statutes
- Common law
  - Tortious invasion of privacy
- Key issue:
  - Whether there was a legitimate expectation of privacy
  - Even if there was a legitimate expectation of privacy, was it outweighed by legitimate business interest

VENABLE LLP

Legal Landscape

- Personal text messages on employer's device
  - Supreme Court case (*City of Ontario v. Quon*, 2010)
  - Held that search of police officer's personal messages (including sexually explicit messages) on a government-owned pager was reasonable and did not violate police officer's constitutional rights under the 4th Amendment
  - Search was motivated by legitimate work-related purpose (whether it needed to modify its wireless contract regarding text messages)
  - Employer policy stated employee communications would be monitored, but supervisor informed employee that they would not audit texts as long as employees paid any over-limit fees
  - Lesson for private employers – legitimate employer interests may trump employees' privacy interests

VENABLE® LLP

Legal Landscape

- Factors courts often use regarding the "reasonable expectation of privacy" determination in the context of email transmitted over employer's server:
  - Does the employer maintain a policy banning personal or other objectionable use
  - Does the employer monitor the use of employee's computer or e-mail
  - Do third parties have a right of access to the computer or e-mails, and
  - Did the employer notify the employee, or was the employee aware, of the use and monitoring policies

VENABLE® LLP

Legal Landscape

- Telephone monitoring
  - Employers may monitor business-related calls (except California law requires that when parties to call are all in California, they be informed when conversation is being recorded)
  - Under federal case law, when employer realizes call is personal, he or she must stop monitoring the call

VENABLE LLP

Legal Landscape

- Computer monitoring
  - Employers can see what is on the screen, stored on computer terminals, stored on hard drives
  - Employers can monitor Internet usage such as web-surfing and electronic mail
  - Company e-mail is owned by company and can be monitored and reviewed
  - Even private e-mails sent from company computer to/from Yahoo, Hotmail, or other web-based accounts can be monitored or reviewed
    - Exception found in one case involving e-mails from employee's personal account with attorney due to attorney/client privilege

VENABLE® LLP

Legal Landscape

- Personal v. Private Device
  - Increasingly, employees are requesting and employers are allowing use of personal devices to be connected to employer network
  - Challenge is determining what is “private”
  - Same analysis of expectation of privacy applies

VENABLE® LLP

Social Media

- When can employer monitor, review, or take action based on employee social media activities
- Certain laws protect employees from being disciplined and fired based on social media posts
  - Labor laws – Section 7 of the NLRA protects "concerted activity" about terms and conditions of employment
  - Whistleblower laws (federal and state)
  - Anti-retaliation laws
  - Off-duty conduct state laws

VENABLE LLP

Social Media

Key: Limit or decrease expectation of privacy (express or implied consent)

- Specific disclaimers waiving right to privacy
  - Inform employees that e-mail should not be considered private
  - Passwords, even if "personalized," are on loan and are property of the company
- Blanket disclaimers in employee handbooks, etc.
  - Company property is for company use
  - Using company property for private use may be cause for discipline
- Notify employees clearly of corporate testing, monitoring and surveillance policies
- Proceed with caution before taking any disciplinary action against employees for violations of social media or Internet use policies (especially personal use)

VENABLE LLP

Policies

- Zero-tolerance policy is not recommended
  - Not realistic, workable, or welcome in today's mobile workforce
- Electronic communication policy must be in place
  - Protect organization's assets
  - Protect reputation
  - Increase productivity
  - Ensure compliance with the law

VENABLE LLP

Policies

- Be specific
  - What type of monitoring
  - Frequency of monitoring
  - Purpose of monitoring
  - Scope of monitoring (including personal e-mails, voicemails, phone calls, video monitoring)
- Filtering of certain websites
- Establish clear security procedures to protect private information
- Establish guidelines regarding use of portable devices such as laptops, BlackBerries, and cell phones

VENABLE® LLP

Policies

- Policy considerations for mixed-use devices
  - Security of information (passwords, encryption, etc.)
  - What type of monitoring will occur of personal devices connected to employer network
  - Access to nonprofit data, information, and other relevant information stored on the personal device
  - What happens in the event of an investigation or litigation
  - How does information from personal device get stored for document retention and destruction purposes
  - Retrieving information when employee resigns or gets terminated
  - Require virus protection
  - What happens if device is stolen or lost
    - "Kill command"
- Consider personal device use agreement, in addition to other policy

VENABLE® LLP

Practical Tips

- Work with IT to wall-off company e-mail on personal devices (i.e., “Good” software)
- Exit interviews
  - Ensure return of property, and information stored on personal devices, external hard drives, cell phones, and other devices before employee leaves

VENABLE LLP

Background Checks

- Emerging issue: increased privacy protections in the background check process
  - Increased protection of applicant information learned through background checks
  - Whether the use of credit history and criminal history constitutes adverse impact discrimination
  - Pepsi Case
    - EEOC's investigation revealed that more than 300 African-Americans were adversely affected when Pepsi applied a criminal background check policy that disproportionately excluded black applicants from permanent employment
    - Under Pepsi's former policy, job applicants who had been arrested pending prosecution were not hired for a permanent job even if they had never been convicted of any offense
    - 3.13 million dollar settlement, and provide job offers and training

Background Checks

- Emerging issue:
  - Lessons from Pepsi
    - EEOC recommends that employers consider:
      - nature and gravity of the offense,
      - time that has passed since the conviction and/or completion of the sentence, and
      - nature of the job sought in order to be sure that the exclusion is important for the particular position

Background Checks – State Laws

- California
  - For all background checks through reporting agency, must add reporting agency's website to authorization form so that individuals can go online and check the agency's privacy policies
  - If doing credit checks, must be job-related and must explain the reason in notice and authorization form:
    - Position is in management
    - Position is in the State Department of Justice, a sworn peace officer, or law enforcement
    - Employer is required by law to consider credit history information.
    - Job requires regular access to bank or credit card account information, Social Security numbers, or dates of birth (but not if access to such information merely involves routine solicitation and processing of credit card applications in a retail establishment)
    - Employee will be a named signatory on the bank or credit card account of the employer
    - Employee will be authorized to transfer money or authorized to enter into financial contracts on the employer's behalf
    - Job affords access to confidential or proprietary information.
    - Job affords regular access during the workday to the employer's, a customer's, or a client's cash totaling at least $10,000

Credit Checks – State Laws

- Maryland – Job Applicant Fairness Act
  - Employers may not use credit report or credit history of applicant or employee to make employment decision including hiring, firing, or determinations about compensation or terms/conditions of employment
  - Does not apply to financial institutions that accept federally insured deposits, credit unions, or investment advisors registered with SEC
  - Employer MAY request credit history post-offer if credit history is substantially job-related and disclosed in writing to the applicant or employee
    - Job-related: managerial (involves direction or control of business or department); access to personal information of customer, employee, or employer (such as social security number, account number); involves fiduciary responsibility to the employer (authority to issue payments, collect debts, transfer money, enter contracts); provided an expense account or corporate credit card; or have access to trade secrets or other confidential business information
- Connecticut, Hawaii, Washington, Oregon, and Illinois have similar laws
- EEOC conducting investigations
- Many other states considering similar legislation
- Proposed federal "Equal Employment for All Act" – similar to CT and MD laws

VENABLE LLP

Background Checks

- Elements
  - Education check
  - Reference checks
  - Criminal background check
  - Social security check
  - Credit check?
  - Google?
- Factors to consider in determining level of check
  - Level of position
  - Level of access to information, funds, and discretionary spending
  - Cost
  - Consistency
- Ensure compliance with Fair Credit Reporting Act

VENABLE® LLP

Background Checks

- What to do with the information
  - Interpretation
  - Relevance
  - Consistent and methodical approach
- Recordkeeping
- Understanding limits of the background check
- Maximizing other parts of the hiring process to make a good hire

VENABLE® LLP

Questions?

Venable LLP
575 7th Street NW
Washington, DC 20004

Jeffrey S. Tenenbaum
jstenenbaum@Venable.com
t 202.344.8138

David R. Warner
drwarner@Venable.com
t 703.760.1652

Grace H. Lee
glee@Venable.com
t 202.344.8043

To view Venable's (searchable) index of articles, events, PowerPoint presentations and recordings on nonprofit legal topics, see www.Venable.com/nonprofits/publications, www.Venable.com/nonprofits/recordings and www.Venable.com/nonprofits/events.

VENABLE® LLP