# Privacy in the Workplace

Jennifer Rubin and Gauri Punjabi

Mintz Levin. **Not your standard practice.**

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Speaker Introduction

**Cynthia Larose**

*Chair*

Privacy & Security

**Jennifer Rubin**

*Member*

Employment, Labor & Benefits

**Gauri Punjabi**

*Associate*

Employment, Labor & Benefits

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Our Privacy & Security Practice

- Interdisciplinary practice serving a wide range of industries
- Advise clients on US federal and state laws related to data protection and data breach notification
- In-depth familiarity with the EU Data Protection Directive and requirements in EU member states and other international jurisdictions
- Thought leadership delivered through our Privacy & Security Matters blog

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Housekeeping Notes

- The webinar will be recorded.
  - The recording and slides will be sent to all participants after the webinar.
- If you are calling in through your computer, please be sure to turn up the computer's volume.
- Questions will be answered at the end of the presentation.
  - Use the Q&A application to submit a question.
- Please be alert for the code required for CLE credit, which we will provide during the course of the webinar

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# What We're Going to Cover

- Statutory and Case Law Developments
- Social Media in the Workplace
- Bring Your Own Device Issues

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Where is your Workplace?

# Privacy in the workplace: Statutory considerations

- Federal Statute
  - Electronic Communications Privacy Act of 1986
  - The ECPA prohibits the intentional interception of "any wire, oral or electronic communication," but includes a business use exemption that permits email and phone call monitoring.
- Two situations where ECPA not violated:
  - Typically, if the employee is using a company computer or device and the employer can show a valid business reason for monitoring the employee's activity (whether it be telephone usage or email), then the employer does not violate the ECPA.
  - If the employee has consented to email or phone monitoring.

# State Law Statutory Developments:

- Currently, Connecticut and Delaware are the only two states that have passed legislation requiring employers provide notice to employees prior to monitoring e-mail communications or Internet access.
  - The Connecticut law, codified at Conn. Gen. Stat. § 31-48d, requires employers who engage in any type of electronic monitoring to "give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur."
  - Delaware's statute, codified at 19 Del. C. § 705, states that an employer may not "monitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either: (1) Provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer-provided e-mail or Internet access services; or (2) Has first given a 1-time notice to the employee of such monitoring or intercepting activity or policies."

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Privacy in the Workplace: Statutory Considerations

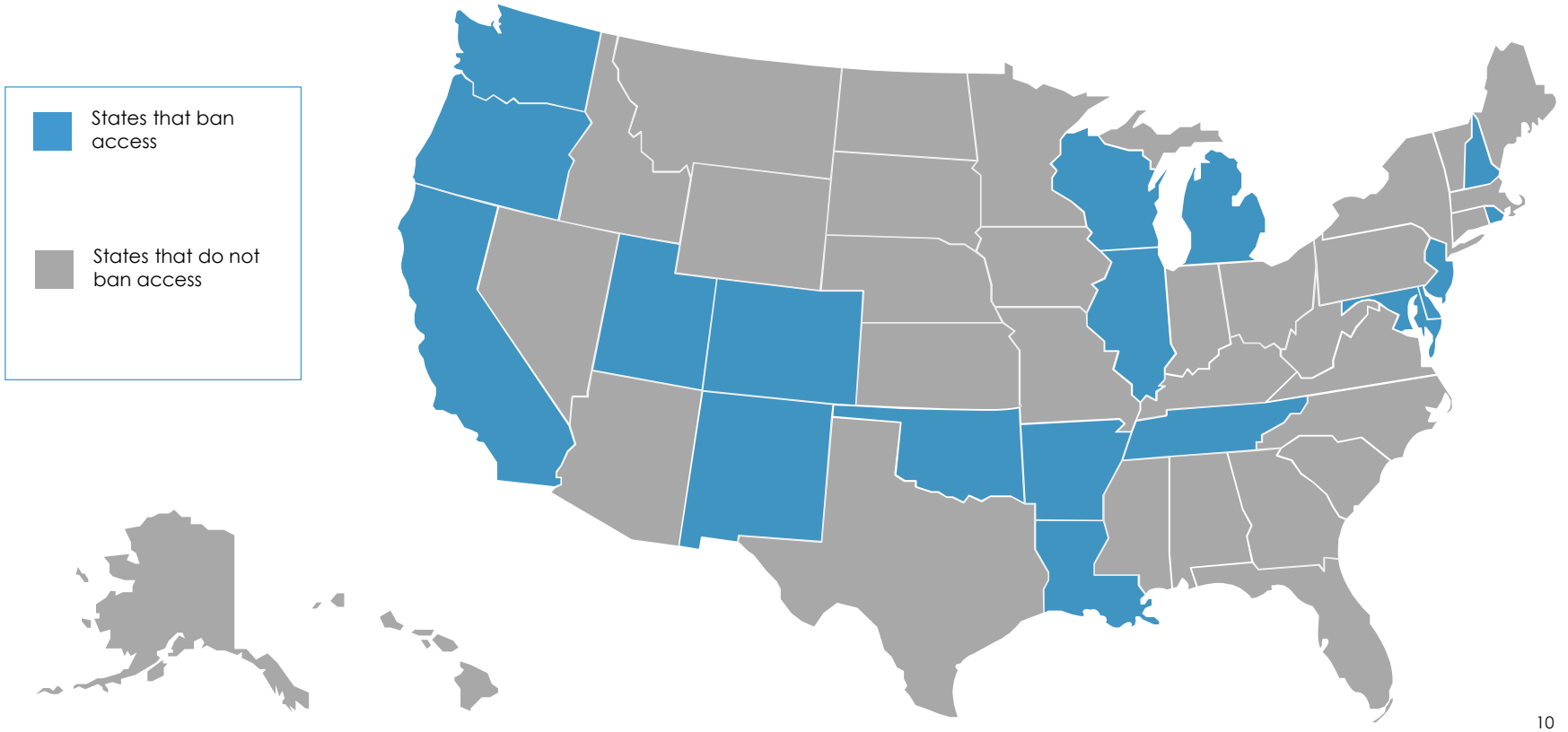
## Statutory Restrictions on Access to Social Media Accounts

On Aug. 1, 2014, New Hampshire became the 18th state in the country to bar employers from requesting access to personal social media accounts of present employees or job applicants

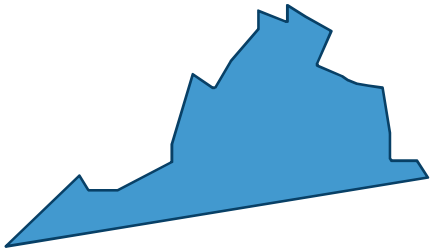
In 2014 alone, six states (Louisiana, New Hampshire, Oklahoma, Rhode Island, Tennessee and Wisconsin) passed social media privacy laws.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

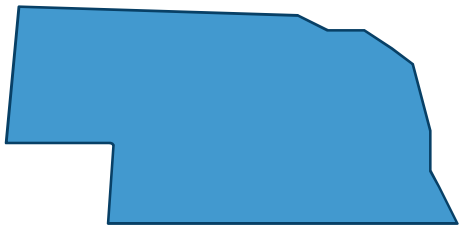
# States that ban employer access to social media accounts



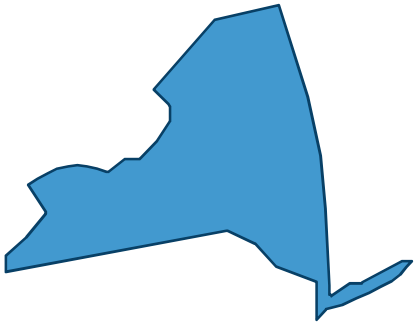
# What are Common Law Privacy Rights in the Workplace?



***Va. Code Ann. § 8.01-40 (2011)).***



**Neb. Rev. Stat. §§ 20-202 to 205.**



**N.Y. Civil Rights Law §§ 50 & 51.**

**Wis. Stat. § 895.50.**

# What are Common Law Privacy Rights in the Workplace? (Cont.)

- In the absence of a state constitutional provision or statute guaranteeing privacy protection, employees must rely on judicially created "common law" protections not derived from statutes.
- Most typically, these "common law" privacy cause of action claims take the form of "intrusion upon seclusion" claims
  - Though it varies from state to state, generally, a plaintiff must establish that:
    - That the defendant, without authorization, intentionally invaded the private affairs of the plaintiff;
    - the invasion must be offensive to a reasonable person;
    - the matter that the defendant intruded upon must involve a private matter; and
    - the intrusion must have caused mental anguish or suffering to the plaintiff.
- In the employment context, it is generally very difficult for an employee to succeed with this claim, particularly in establishing the second element because there is generally a lowered expectation of privacy in the workplace.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Common Law Developments

Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 661 (D.N.J. 2013)

- Plaintiff worked as a registered nurse and paramedic at a nonprofit hospital service corporation (MONOC). Plaintiff maintained a Facebook account and selected privacy settings for her account that limited access to her Facebook wall to only her friends. Plaintiff did not add any MONOC managers as Facebook friends but did add a MONOC paramedic named Tim Ronco. Unbeknownst to Plaintiff, Ronco was taking screenshots of Plaintiff's Facebook wall and printing them or emailing them to a MONOC manager.
- Plaintiff posted the following statement to her Facebook wall:
  - An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards....go to target practice.

# Common Law Developments (Contd.)

Ehling, continued

- After MONOC management was alerted to the post, Plaintiff was temporarily suspended with pay, and received a memo stating that management was concerned that Plaintiff's comment reflected a "deliberate disregard for patient safety." Plaintiff also filed a complaint with the NLRB. The NLRB found that MONOC did not violate either the NLRA or her privacy. After Plaintiff brought suit a New Jersey district court agreed and found no privacy violation since the post was sent to management unsolicited.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Common Law Developments (Contd.)

Roberts v. CareFlite, 2012 Tex. App. LEXIS 8371 (Tex. App. Oct. 4, 2012)

- Plaintiff worked as a paramedic and was Facebook friends with two coworkers, a fellow paramedic and a helicopter pilot. Plaintiff posted on her pilot coworker's wall that she had transported a patient who needed restraining and that she wanted to slap the patient. After the employer was notified of the post, it terminated Plaintiff for, among other things, unprofessional behavior. The court later dismissed Plaintiff's invasion of privacy claim finding Plaintiff had failed to establish any invasion of her privacy since third parties could view her post.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# NLRB Decisions

- NLRA Section 7 and Section 8(a)(1) protect "concerted activity."
- NLRA applies to all employers whether or not a workplace is unionized.
- In 2011 and 2012 , the NLRB's General Counsel issued three memos on employer social media policies.
- Recent series of NLRB decisions apply strict standard.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# NLRB Ruling: Protecting Group Action

Triple Play Sports Bar and Grille, Nos. 34-CA-012915, 34-CA-012926 (N.L.R.B. Aug. 22, 2014).

- A policy in the employer's handbook stated that employees were subject to discipline if they used social media to "engag[e] in inappropriate discussions about the company, management, and/or co-workers."
- NLRB:
  - Clicking the "like" button could constitute protected activity.
  - The policy violated the NLRA

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# NLRB Ruling: Protecting Group Action

Purple Communications, Inc. and Communications Workers of America, AFL-CIO, Nos. 21-CA-095151, 21-RC-091531, 21-RC-091584 (N.L.R.B. Dec. 11, 2014)

- Employees with access to an employer's email systems have the right to communicate with each other during non-working time via the employer's email system to engage in statutorily protected communications, such as discussing wages, hours, conditions of employment and union organizing.
  - Decision significantly limits employer's ability to control the use of its devices

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Avoid Broad Definitions

Hoot Winc, LLC, No. 31-CA-104872 (N.L.R.B. A.L.J. May 19, 2014)

- Handbook prohibited "insubordination to a manager or lack of respect and cooperation with fellow employees or guests." A server was terminated for violating the rule by posting disparaging comments about coworkers and managers on social media.
- ALJ: "Insubordination rule" violated NLRA.

Lily Transp. Corp., No. 01-CA-108618 (N.L.R.B. A.L.J. Apr. 22, 2014)

- Handbook provided "employees would be well advised to refrain from posting information or comments about [the company], [the company's] clients, [the company's] employees or employees' work that have not been approved by [the company] on the internet."
- ALJ: NLRA violation because rule not "restricted to confidential or even company information."

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Employees' Personal Computers

Prof'l Elec. Contractors of Conn., Inc., No. 34-CA-071532 (N.L.R.B. A.L.J. June 4, 2014)


- Handbook prohibited "[i]nitiating or participating in distribution of chain letters, sending communications or posting information, on or off duty, or using personal computers in any manner that may adversely affect company business interests or reputation."
- ALJ: Rule violates NLRA
  - "insofar as it prohibits employees from using their own computers to communicate with others 'in any manner that may adversely affect the company business or reputation.'"

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Employers Not Powerless

## Landry's Inc., No. 32-CA-118213 (N.L.R.B. A.L.J. June 26, 2014)

- Handbook stated "the Company ***urges*** all employees not to post information regarding the Company, their jobs, or other employees which could lead to morale issues in the workplace or detrimentally affect the Company's business."
- ALJ: Focusing on the use of word "urge," finding that policy passes muster.

## Richmond District Neighborhood Center (Case 20-CA-091748, October 28, 2014)

- No written policy. Employees engaged in profane Facebook discussion advocating various insubordinate acts, neglecting job duties and encouraging students to write graffiti on walls.
- NLRB: The employees lost the NLRA's protections.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Social Media Policies

- What is a Social Media Policy
  - A policy, typically written and distributed to employees, that outlines the employer's expectation of acceptable use of social media by its employees.
- Why Have a Policy?
  - Employer may clearly and uniformly articulate its expectations of social media use to employees
  - Provides direction to employees and aids in safeguarding against social media mishaps

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Social Media Policies

- Issues
  - Technology constantly evolving, making it difficult for companies' social media policies to keep up
    - For example, a relatively new application aimed at professionals, Confide, allows users to send each other messages, including photos and documents, which disappear after they're read.
    - Does your  policy address any potential issues raised by the app?
    - How does an employer exercise control over this technology? Should it?

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Recruiting

- Use of social media in recruiting
  - LinkedIn, Facebook, Google …. What does this information return to the employer?
  - Impacts Title VII, the ADA, ADEA, and all the state counterparts …. Because now you have information that may not have been disclosed on the resume
  - Fair Credit Reporting Act issues

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# What is BYOD?

- Bring Your Own Device (BYOD)
  - Employers are moving towards permitting employees to bring personally owned mobile devices (laptops, tablets, smart phones, etc.) to the workplace and use those devices to access company information and applications.
  - Estimated that 60% of white collar workers use a mobile device for work purposes
  - 40% of all white collar workers own the smartphone they use for work

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Benefits of BYOD Policies for Employers

- Improved employee productivity
- Greater job satisfaction for employees
  - Studies show employees prefer using their own devices rather than a company-issued device, which is typically outdated.
- Lower costs (related to device overhead)

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Issues Raised by BYOD Policies for Employers

- Concerns over employee privacy and the extent to which an employer may access or monitor an employee's device
- Security concerns over protection of proprietary information and data breaches
- Legal implications
- What to do when an employee leaves the company?

# Employee Privacy

- BYOD policies create an inherent tension between the company's interest in monitoring and accessing an employee's device and the employee's expectation of privacy in the use of their device.
  - Potential Scenarios:
    - A company's mobile device management system enables it to monitor activity, track, and remote lock and wipe an employee's personal device. Does the company's practice potentially violate an employee's privacy rights?
    - An employee uses a personal laptop for business purposes consistent with the company's BYOD policy. When the employee's laptop is stolen, will issues arise if the company executes a remote wipe of the device, resulting in the loss of all of the employee's personal data on the phone (family photos, text messages, etc.)?
    - An ex-employee sues his former company and during discovery company seeks a forensic examination of work-related items on employee-owned devices. Will concerns arise if the employee was never made aware of this possibility?

# Security Concerns and BYOD

- Arguably, the greatest concern raised by remote devices for employers relates to protecting proprietary information and potential security breaches.
- These concerns are even more present where employers utilize a BYOD policy, because the employee's device will contain both personal data, most troublingly in the form of apps, and company proprietary data.
  - In a recent study, IBM found that 50% of employee BYOD devices contained social media dating apps. IBM then reviewed 41 smartphone dating apps available for Google's Android and discovered potential security risks in 26 of the 41 social media apps. The identified risks meant the apps could be used to download malware or steal information.

# Departing Employees and the Remote Wipe

- Outgoing employees utilizing a company's BYOD policy present a particular problem.
- Many employers, 21% according to a recent survey, perform remote wipes when an employee quits or is terminated.
  - Smart employers implement and promulgate BYOD policies that specifically address what happens when an employee leaves or is terminated.
  - In addition, current software allows companies to only remove work-related material from a smartphone or computer and companies could avoid potential headaches by utilizing such technology.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Legal Implications: Is the employee on the clock?

- Under the Fair Labor Standards Act (FLSA), non-exempt employees must be paid overtime compensation for any hours worked in excess of 40 hours in any workweek.
- For non-exempt employees, compensable time includes any time spent on devices responding to work emails or performing company work outside the employee's regular schedule.
- Mobile devices, particularly personal devices, enable employees to potentially perform work at anytime, anywhere, because the employee is always accessible to the company.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Have a Policy

- Despite the very serious implications raised by implementing a BYOD policy, many companies neglect to provide a policy to employees regarding access to an employer's network from mobile devices
  - Only 50% of enterprises and 41% of midsize firms have a policy in place regarding employee network access for mobile devices.
  - Less than half have policies about mobile transmission of company data.
- Make sure it covers the bases:
  - Acceptable use;
  - Security;
  - Employer monitoring;
  - Policy for outgoing employees and lost devices

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Takeaways - BYOD

- Benefits of effective training and implementing a BYOD mobility policy that employees are required to sign:
  - Manages employees' expectations
  - Communicates company's legitimate concerns
  - Notifies employees that their privacy rights are impacted
- The price for failing to address these issues through effective policies and employee training can be steep:
  - In January 2014, a U.S. federal judge in Illinois sanctioned pharmaceutical manufacturer Boehringer Ingelheim more than $900,000, in part, because the company did not ensure its employees saved work-related text messages on their personal phones after litigation had commenced.
  - In a recent survey, 42% of executives said a mobile security incident generally costs more than $250,000.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# An Employer's To-Do List

- Know your jurisdiction's requirements when it comes to employee privacy rights
  - Consider any applicable statutes and case law
- Have a social media policy, but know the limits and don't go too far
- Weigh the costs and benefits to implementing a BYOD policy

# Questions?

Thank you for joining us!

Subscribe to our blogs for updates and analysis:
www.privacyandsecuritymatters.com
www.employmentmattersblog.com

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Cynthia J. Larose, *Member*

- Boston University (JD)
- Boston University (MS)
- University of Massachusetts (BA)

- Chair of the firm's Privacy & Security Practice and a Certified Information Privacy Professional (CIPP)
- Represents companies in information, communications, and technology, including e-commerce and other electronic transactions
- Has extensive experience in privacy, data security, and information management matters
- Is a frequent speaker on privacy issues at conferences and media appearances and presents privacy awareness and compliance training seminars to client companies

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Jennifer B. Rubin, *Member*

- University of Connecticut (JD)
- University of Connecticut (BA)

- Focuses her bi-coastal C-suite executive compensation practice on meeting the increasingly complex employment needs of executives of public and private corporations
- Leverages her twenty-five years of experience as a trial lawyer to help clients craft business solutions to legal problems
- Focuses practice on solving employee mobility issues, litigating wage and hour class actions, and making employment regulations accessible for her corporate clients

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Gauri P. Punjabi, *Associate*

- University of Notre Dame (JD)
- Northeastern University (BS)

- Practice covers the full scope of employment law issues and encompasses a wide range of industries, including hospitality, nonprofit organizations, technology, and health care
- Regularly represents clients in employment related litigation, including non-compete and trade secret issues, employment contracts, and discrimination claims.
- Counsels clients throughout the entire process from the initial filing through representation in the courts