Mobile Devices in the Workplace: What Every Employer Needs to Know

Presented by:
Shannon Huygens Paliotta
Senior Associate, Littler Mendelson, P.C.
spaliotta@littler.com
(412) 201-7631

Marcy McGovern
Knowledge Management Counsel, Littler Mendelson, P.C.
mmcgovern@littler.com
(412) 201-7623
SURVEY: How Mobile is Your Workforce?

- How many employers issue, and pay for, smartphones or tablets to employees for work use?
- How many employers have rules dealing with when and how devices can be used away from work?
- How many employers actively monitor work-related smartphone or tablet use away from work?
How Mobile Is Your Workforce?

- Even if your company doesn’t issue smartphones, your employees are using them for work – and working on average **240 more hours per year** than their non-mobile counterparts.
- **53 million** full-time American employees own smartphones
- As a result of BYOD (“Bring Your Own Device”) Policies:
  - **90%** of American workers use their personal smartphone for work
    - **70%** of employees in financial services industry
    - **95%** of employees in education industry

What do you do when you first wake up?

Among All Respondents
- 79% reach for phone within 15 minutes of waking
- 62% reach for it immediately after waking
- 44% reach for it immediately & use as alarm clock

Among 18-24 year olds
- 89% reach for phone within 15 minutes of waking.
- 74% reach for it immediately after waking
- 54% reach for it immediately & use as alarm clock

Always Connected, IDC Study, Sponsored by Facebook, March 2013
How is Your Workforce Mobile?

• **After Hours:**
  – 70% of employees who use smartphones for work are expected to read emails before or after normal working hours

• **On Weekends and Vacation:**
  – 72% of Americans check their email on weekends, vacation or other days off
  – 30% expect to read work-related emails on summer vacation

Is Your Company Keeping Up With Technology Trends?

Most Employers Choose One of Two Options:

1. Provide mobile devices and service for employees over which the company maintains ownership and control.

2. Allow employees to purchase mobile devices and service that gives them access to work-related resources, subject to company BYOD program.
Advantages of Employer Owned Devices

• Employer controls what software, programs, applications, etc., can be used on the device.
• Employer controls the security of any and all work-related data transmitted and saved.
• Employer can collect the device and all secured information on the device if an employee leaves.
• Employer controls all potentially relevant electronic discovery on device.
Disadvantages of Employer Owned Devices

- **COST** – both of the initial set up and upgrading devices as technology advances
- High level IT commitment to investigating, purchasing and maintaining devices, applications, security, etc.
- Defining what is acceptable personal use for employees
Advantages of BYOD

- Employee Convenience of All-In-One Device
- Employee Can Choose Best Device for Needs
- Improved Employee Engagement
- Increased Flexibility
- Increased Productivity (?)
- Lower Costs (?)
Challenges BYOD Programs Must Address

- Security of Company Data
- Records Management
- Trade Secrets and Confidential Info Held By Former Employees
- Wage &Hour and Reasonable Accommodation Issues
- Litigation and eDiscovery
- Employee Privacy Rights
Security Dangers of Mobile Devices

• Lost or Stolen Devices
  • Accounts for 31% of security breaches
  • Data stolen by friends/family makes up 25% of reported incidents

• Malware / Viruses
  • 52% of full-time employee participants in BYOD programs access unsecured WiFi networks

• Records Management/Retention
  • Who has what data?
  • When and how is it destroyed?
What Are Your Employees Sending to the Accidental Cloud?

- Mobile devices send information to data storage, video, photography and social networking sites, and web-based email providers
- Cloud services can replace thumb drives for storage
- Cloud services also provide collaboration capabilities – may be used to circumvent IT restriction on sharing information outside the enterprise
- Third party storage: Where is your data?
  - iCloud
  - Google Docs
  - Dropbox.com
  - Box.net
- Generally, there is no reasonable expectation of privacy in data held by third parties
- An employer rarely has any control over data stored by third party providers
What Happens When An Employee Leaves?

BYOD Environments Raise **Two Important Issues:**

1. Who controls the data stored on an employee owned device at the time of termination?

2. How does an employer monitor what information the employee may have sent or saved to a personal account from that device before leaving?

In 2008, the Economist reported that 60% of American workers took some employer data with them after they left. Imagine what that number looks like in today’s mobile workforce.
The 24/7 Workforce

*Allen v. City of Chicago*, (N.D. ILL. 2013)

-Collective action brought by hourly employees alleging failure to pay overtime for off-duty time reading and responding to email on city-issued Blackberries.

• Do your hourly, non-exempt employees have access to company systems on their mobile device?

• Are you monitoring their access to ensure they are not performing any work after hours for which they are not being compensated?

• Are your employees feeling any pressure from managers to respond to work-related issues after hours?
Reasonable Accommodations

• Yahoo recently made headlines when its CEO abolished the company’s work-from-home policy
  – Cited problems with morale, innovation, and collaboration
  – Sparked debate over workplace flexibility

• EEOC’s view: Working from home is a reasonable accommodation under the ADA
  – Guidance: “Changing the location of where work is performed may fall under the ADA’s reasonable accommodation requirement of modifying workplace policies, even if the employer does not allow other employees to telework.”
Litigation and eDiscovery Issues

• Identification of BYOD devices/information subject to a litigation hold.

• Practical challenges of data collection, do you have technical capability to collect data from employee’s chosen device?

• Who has “ownership and control” of the data on the devices? What about possibly incriminating evidence like photos, text messages, pornography?

• Will employees be required to produce mobile devices to employer for inspection, preservation and production?

• Will employees be required to allow access to other home devices such as storage devices, or Cloud-based storage accounts that may have been “synced” with their device?
Threshold Questions

• Who will participate in any BYOD program?

• What policies and security measures need to be established based on the programs used by your employees?

• What current policies, procedures, or job descriptions need to be updated to account for a BYOD program?
  – For example: Harassment, Workplace Safety, Time Recording and Overtime, Compliance and Ethics, Records Management, Confidentiality, etc.
Threshold Questions Cont.

- What contracts or other agreements might you need with employees to protect confidential, trade secret, customer, employee or protected health information?

- What vendor relationships will you need to engage in order to establish and maintain a BYOD program?

- Do you need to bargain any terms under a current labor contract?

- How will you comply with the FLSA and other state wage and hour laws?

- How will you address telecommuting and reasonable accommodation issues?

- How will you ensure the company is equipped to defend itself in any forthcoming litigation?
Setting Up a BYOD Program:
Which employees can participate in the program?

• **Who participates in program?**
  
  – Limit to exempt employees to reduce exposure to “of the clock” claims.
  
  – If non-exempt employees are included, need to address overtime wage exposure.
  
  – Exclude contractors and contingent workers who may be working for other customers.
  
  – Consider excluding individuals who handle sensitive information.
  
  – Consider excluding individuals in sensitive positions or involved in litigation or regulatory proceedings.
What is MDM – Mobile Device Management?

Mobile Device Management:

- Software that allows corporate IT to manage use of mobile devices. Component of BYOD programs. Features may allow an employee to:
  - Require users to register device as condition of network access
  - Lock down end user’s ability to use specific device features or apps, such as cameras, Siri or iCloud
  - Enable remote locking or wipe of device
  - Enforce use of strong passwords
  - Implement anti-spam solutions – Siri, iCloud file sharing, blacklists
  - Prevent users from disabling or altering security settings on devices
Additional Security Recommendations

• Restrict employees from using cloud-based applications, cloud-based backup, or synchronizing with home PCs or other devices for work-related data
• Specifically prohibit employees from allowing friends or family members from using their devices
• Revise your exit interview process to remove all company data remaining on a terminated employee’s device
• Require strong passwords
• If device is sending location-based information, disclose the practice. Tread carefully to avoid allegations of unlawful surveillance
Setting Up a BYOD Program

• Address tradeoff of privacy for convenience up front:
  
  – Participation in program is a privilege, not a right
  
  – Require employees to consent to the company’s access of its data on the device as a condition of participation.
Three Approaches to Separation of Personal & Professional

- Virtualization: remote access to corporate network so that corporate data and applications are not stored on the device
- Sandbox/Walled Garden: separate business application provides secure application segregated from personal data
- Separation by Policy: corporate and personal data are commingled and use combination of policy and IT controls for security
Privacy Parameters

- Distinguish between data and device
- **Device**
  - May require return upon demand or inspection as part of investigation
  - May require return, with data intact, upon separation from employment
- **Data**
  - Determine whether employer will retain right to review all contents of device or will exclude categories such as music and photos
  - Require employee to provide access to cloud backups or home server?
  - Monitor/limit employee’s use of web-based applications? Example: Siri, Dropbox, iCloud, etc.
  - Set parameters for timing, terms and extent of remote wipes
Protection of Trade Secret Information

- Take Reasonable Measures to Protect Trade Secrets in a BYOD Environment
  - Non-competes, NSAs, etc.

- Use Confidentiality Agreements/Proprietary Information Assignment Agreements ("PIAA")
Breaking Up is Hard to Do:
Clarify your right to wipe devices and ownership of social media assets before the breakup

• Tell employees that their company issued electronic devices will be “scrubbed” or “wiped” in the event of termination and get written acknowledgement.

• Clarify ownership of data stored on a company sponsored mobile device.

• Maintain access to, and right to change, passwords to corporate accounts.
Terry is an IT administrator with your company. Sadly, Terry is suffering from late-stage renal failure and requires daily kidney dialysis. Terry asks to work from home (where he has a home dialysis machine) as a reasonable accommodation, which you have done in the past for a help desk IT employee and your billing coordinator. You are concerned about this request because Terry’s duties occasionally require him to be physically present in the office to install equipment.
须你允许Terry在家工作？

a) 它取决于他的工作描述/基本工作职责。

b) 它取决于你如何处理其他员工请求在家工作的要求。

c) 它取决于他的请求是否会为公司其他IT管理员造成不当的困难。
Your company’s BYOD policy is popular with employees. A sales employee, Susan, loves to use her iPhone 5 to send and receive work emails. Based on the nature of her job, Susan’s emails often contain confidential information and trade secrets. Susan also maintains an extensive database of sales “leads” in her phone’s contacts. You have just learned that Susan resigned and is leaving for a competitor. The IT Department wants to remotely “wipe” her iPhone.
A FEW HYPOTHETICALS

• What concerns do you have about IT’s request?

• What litigation issues does this present?

• What policies/procedures/or other measures could have prevented this dilemma?
Sarah is a non-exempt secretary with your company. Because your company has operations on the East and West Coast, Sarah prefers to log into your Citrix environment to access her work email account from home at night to catch up on any emails she may have received from the West Coast so as to feel prepared going into work the next day.

She does not respond to any of the emails and otherwise does not do any work for the company – she just checks to see what is going on.
No one from your company has told Sarah that she needs to do this and she is not submitting overtime requests for checking her email at night as she believes that it is helping her personally to feel more prepared for the next day. As the HR Manager for the division of the Company that Sarah works in, IT sends you an email with her Citrix logs pursuant to their policy to do so when they see frequent logins at night by a non-exempt employee.

- What concerns do you have about Sarah’s conduct?
- What litigation risks does this present?
- How do you plan to reconcile the situation?
BEST PRACTICES FOR AVOIDING LIABILITY

• Understand how your organization is using mobile devices and which job positions could benefit from a BYOD program

• Develop a strategy for managing mobile risks, including:
  – Create a multi-disciplinary team to identify concerns specific to your industry and workforce
  – Continuously evaluate the impact of new mobile and social technologies on the workplace
  – Continuously evaluate the impact of new laws and court decisions on existing policies
  – Update existing policies

• Continue to monitor cost savings, productivity and risks to see if a BYOD program is right for you.
Questions?
Mobile Devices in the Workplace:
What Every Employer Needs to Know

PHRA Annual Conference
October 16, 2013

Shannon H. Paliotta, Esq.
spaliotta@littler.com
Marcy McGovern, Esq.
mmcgovern@littler.com
(412) 201-7600