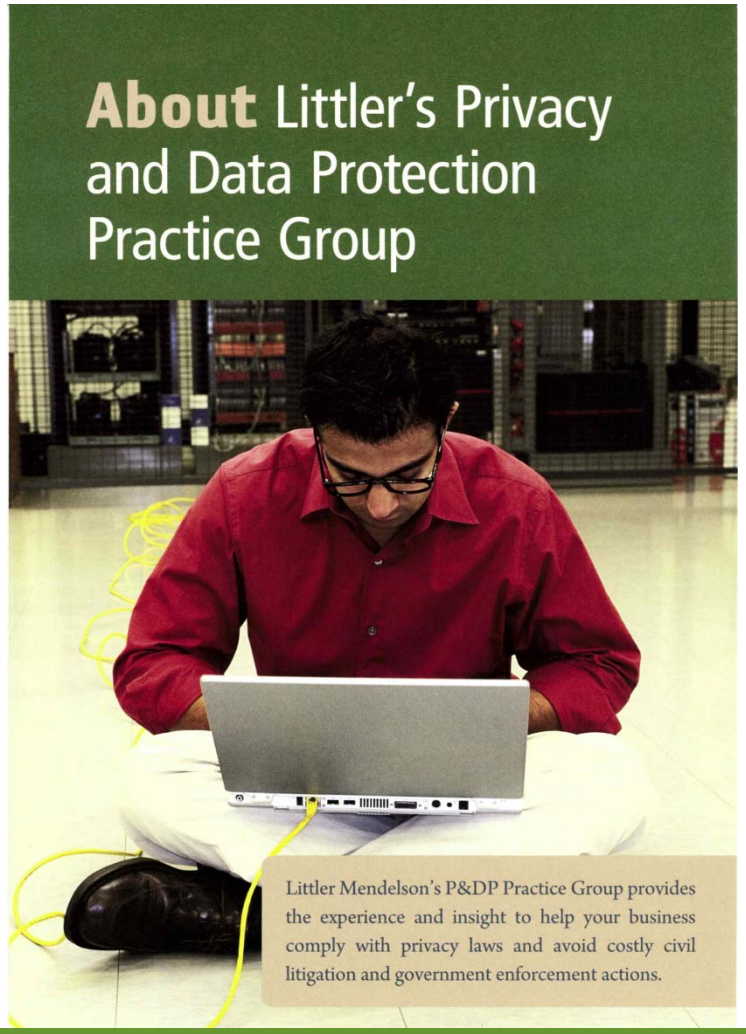
Business Or Pleasure: The Challenges Of Bring Your Own Device Policies In The Workplace

PRESENTED BY

Earl (Chip) M. Jones— Littler, Dallas
ejones@littler.com
(214) 880-8115

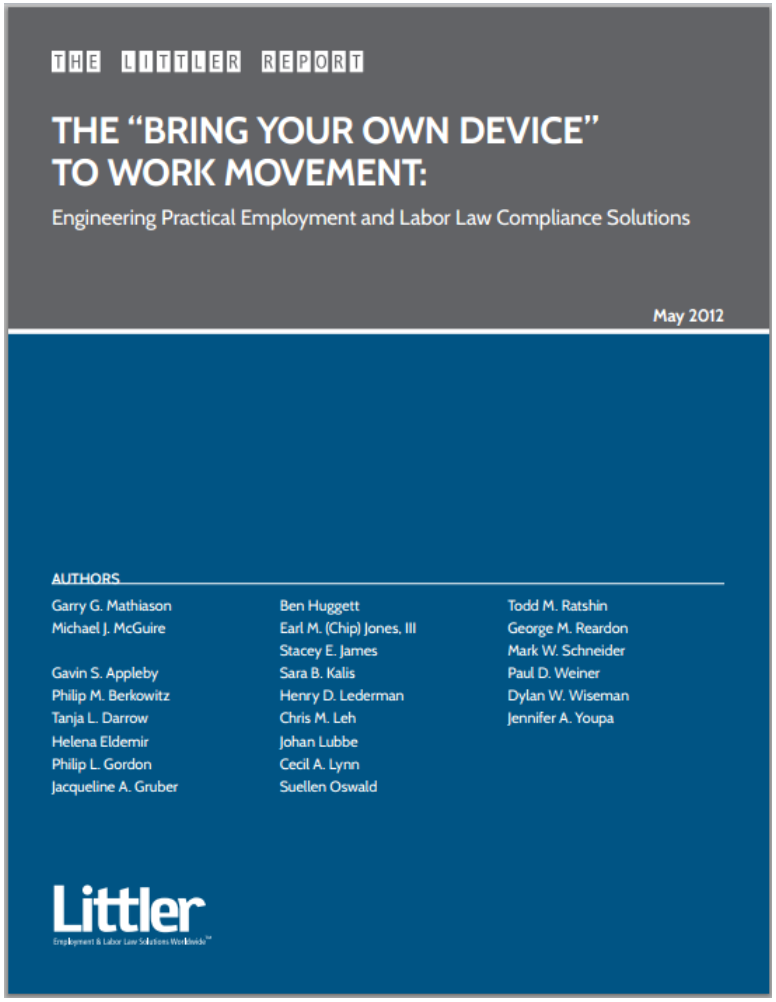
Michelle B. Brookshire— Littler, Dallas
mbrookshire@littler.com
(214) 880-8119

Littler at a Glance



- Littler is the world's largest law firm exclusively devoted to representing management in employment and labor law matters.
- Privacy and Data Protection Practice Group
- Compliance and Ethics Practice Group
  - Investigations
  - Designing incident management systems
  - Analyzing Risk
  - Policy and Procedure Development
  - Training and Education
  - Legal research

Your experiences with BYOD



- What approach has your company taken to the BYOD issue?
  - Restricts to company-owned devices
  - Allows some employees to connect personal devices but process is ad hoc
  - Has a BYOD policy

Why does it matter?

- Conflict between individual rights and organizational obligations
- Ownership of the device most important factor
- Also, affects the employer's ability to control the device and the data

Who's Doing It?

- **IBM**
  - 80,000 employees
  - IBM CIO:
    - "If we didn't support them, we figured [employees] would figure out how to support [the devices] themselves.
- **Kraft**
  - 800 employees receive stipend to buy PC
  - Not available to:
    - company executives who handle confidential information
    - Legal
    - HR staff
    - Employees who use their PC to run production equipment
    - Factory Workers

Why?

- Reducing expenses for employers
- Improving employee engagement
- Aiding in the recruitment of new employees
- Solving the “two pocket problem”
- Innovation to reduce cost and promote collaboration

Ethics and Compliance Issues

Be aware of the culture

Do you feel it is acceptable to...?	Active Social Networkers	Other U.S. Workers
“Friend” a client/customer on a social network	59%	28%
Blog or tweet negatively about your company or colleagues	42%	6%
Buy personal items with your company credit card as long as you pay it back	42%	8%
Do a little less work to compensate for cuts in pay or benefits	51%	10%
Keep a copy of confidential work documents in case you need them in your next job	50%	15%
Take a copy of work software home and use it on your personal computer	46%	7%
Upload vacation pictures to the company network or server so you can share them with co-workers	50%	17%
Use social networking to find out what my company’s competitors are doing	54%	30%

HR and Employment Law Issues

HR and Employment Law Issues

- Performance management
- Discrimination, hostile work environment, accommodation issues
- Workplace Safety
  - Driving and talking or texting
- Labor
  - Mandatory bargaining
  - Unlawful surveillance
- International
  - Data protection
  - Border searches
  - Espionage

HR and Employment Law Issues

- **Wage & Hour**
  - Off-the-clock work by non-exempt employees
  - "Suffered or permitted to work"
  - De minimis?
  - Emails themselves are evidence of time spent and notice to employer
  - Time spent dealing with IT issues related to devices
  - Work by non-exempt *or exempt* employees during weeks off or leaves of absence

HR and Employment Law Issues

- **Solution to W&H Concerns**
  - Prohibit non-exempt employees from accessing email or making work-related calls outside of work
  - Limit access/program participation to employees who are exempt from OT
  - Create process for reporting work performed outside of working hours
  - Training
    - Employees
    - Managers
  - Compliant policy requiring pay for all hours worked

Privacy/Security Issues

Data is heavily regulated

- Security Laws and Regulations
  - Encryption
  - Breach notification
  - Secure data destruction
- Employee privacy rights
- Record retention
- Contractual obligations
  - Indirectly regulated
- Trade secret protection
- eDiscovery obligations

Allowing employees to store company data on their own devices fundamentally complicates these obligations

Security for company data

- **Loss or theft of devices**
  - lost and stolen equipment accounted for 31% of breaches
  - Lookout helped 9 million people locate their devices; one locate request every 3.5 seconds
- **Malware**
  - “malware targeting the Android platform rose 3,325 percent” (Juniper)
- **Friends and family**
  - 27.5% of FINCEN suspicious activity reports involving identity theft involved friends, family, employee in home

Employee Privacy Rights

Access to private information

- GINA
- Protected Characteristics

Issuing a remote wipe command

- Employees have a reasonable expectation of privacy in their personal device
- All 50 states have computer trespass laws
- Computer Fraud & Abuse Act if the unauthorized access causes damages > $5,000

Accessing an employee's personal e-mail or cloud account

- Stored Communications Act
  - *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*

Beware of Computer Trespass

- **Key facts:**
  - Sitton used his personal computer to conduct business for PDI and for a competing business
  - Sitton used the computer on PDI's premises and connected it to PDI's network
  - When PDI caught wind of Sitton's disloyalty, a senior manager entered his office, clicked on an e-mail list, and printed incriminating e-mail

Beware of Computer Trespass

- **Ruling:** Affirms denial of Sitton's claims for computer trespass, computer theft, and computer invasion of privacy
- **Reasoning:** Lack of authority is an element of each claim, and PDI's computer use policy established the manager's authority
- **Key Policy Provisions:**
  - Policy was not limited to company-owned equipment
  - Informed employees that PDI would "inspect the content of computers … in the course of an investigation triggered by indications of unacceptable behavior."

Sitton v. Print Direction, Inc., 2011 Ga. App. LEXIS 849 (Sept. 28, 2011)

Federal Stored Communications Act

- Prohibits unauthorized access to an electronic communication in electronic storage at an electronic communications service provider (18 USC §2701(a))
- Criminal statute with civil remedies
  - Minimum monetary damages of $1,000
  - Punitive damages and attorneys fees
- Consent of the account holder is a defense

Access to Personal E-mail

Key Facts:

- Pure Power Boot Camp fired Fell
- Fell started a competing business
- PPBC's owner (Brenner) accessed three of Fell's personal e-mail accounts
  - Hotmail: Fell had accessed the account using PPBC's computers, leaving username and password behind
  - Gmail: username and password found in the Hotmail account
  - Warrior Fitness Boot Camp: "lucky guess" same password and username
- PPBC used Fell's personal e-mail for non-compete action against Fell

Access to Personal E-mail

- **Claim:** PPBC violated the SCA
- **Defense:**
  - Electronic resources policy defeated any expectation of privacy
  - Fell implicitly consented by leaving username and password on PPBC computers
- **Court: summary judgment for Fell**
  - The policy addressed only company equipment used during the employment relationship
  - The e-mail in question were not created on, sent through, or received from PPBC's e-mail system
  - At most, Fell consented to Brenner seeing his password for one account, but not to her using it for any of them

Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp.2d 548 (S.D.N.Y. 2008)

The Proverbial “Rock and the Hard Spot”

Trade Secret Protection

- "60 percent of American workers who left their employers [in 2008] took some data with them." (Economist)
- Misappropriation may be harder to prove
- Use or disclosure will be the focus
- Access to the devices will be a challenge

eDiscovery Challenges

- Locating the data
- Access to the device
- Collection challenges

Recommendations

Recommendation:

Decide whether all employees should be permitted to participate in a BYOD program or whether certain groups should be excluded.

Who Should Be Eligible?

- **Limit to employees with a business need**
- **Important to control eligibility**
  - The more people with BYOD, the greater the risk
- **NOT employees with regular access to sensitive information**
  - Legal, HR
  - Access to highly valuable trade secrets, *e.g.* product engineers
  - Access to highly sensitive, non-public financial information, *e.g.*, CFO's group
- **Non-exempt employees raise off-the-clock issues**

Recommendation:

Install Mobile Device Management software on dual use devices.

Sandbox Approach

Recommendation:

Require employees to consent to all company activities involving the personal device.

Employee Consent

Consent to:

1. Access to information stored on the personal device
2. Remote wipe of the device
3. Monitoring the device when accessing corporate information

- **Expect Pushback**

Recommendation:

Modify or Create Personal Device Agreements.

The Personal Device Agreement

Critical Terms: Protection against computer trespass, invasion of privacy and other claims

1. Agree to Company's use of remote wipe
2. Agree to Company's monitoring of personal device when connected to the corporate network
3. Agree to produce the personal device for inspection in response to a legitimate requests
4. Release Company from any liability for destruction, or incidental viewing, of personal information

Personal Device Agreement

Additional Terms

6. Will install corporate security package
7. Will not modify corporate security package
8. Will immediately report loss or theft of device
9. Will limit storage of corporate information
10. Acknowledge that all company policies apply to the dual-use device

Recommendation:

Restrict employees from using cloud-based apps, cloud-based backup, or synchronizing with home PCs for work-related data.

Recommendation:

Ensure that use complies with Wage and Hour obligations by prohibiting off-the-clock work and ensuring pay for all hours worked.

Recommendation:

No use by friends and family members.

Recommendation:
Educate and Train

Training

1. Don’t leave the device unattended
2. Don’t share the device’s passwords with anyone
3. Don’t share the device with anyone, including family and friends
4. How to report a lost or stolen device
5. Beware of downloaded apps

Security Incident Response

1. Confirm that dual-use device is encrypted
2. Confirm that remote wipe was activated promptly
3. Confirm that unauthorized acquirer had to unlock a password-protected screensaver
4. If no confirmation, collect e-mail on corporate exchange server from date the loss/theft occurred
   - Search for trigger PII
5. Interview employee concerning contents of local storage on dual-use device

Recommendation:

Revise exit interview processes.

Bottom Line: BYOD creates risks and challenges for employers

- Data-Related Risks
  - Security of company data
  - Privacy of employee data
  - Records management
  - Contractual obligations
  - eDiscovery
  - Trade Secret Protection
  - Contingent Workers
- HR-Related Risks
  - Performance management
  - EEO
  - Wage & Hour
  - Workplace Safety
  - Labor
  - International

Questions

Thank You