


**PLUNKETT COONEY**  
ATTORNEYS & COUNSELORS AT LAW

**BYOD 2.0**

Upgrading Your Knowledge About  
Employee Personal Technology  
Use in the Workplace

Presented by  
**Courtney L. Nichols**  
**Jason G. Bulbuk**




---

---

---

---


---

---


---

---

**Today's Presenters**



Courtney L. Nichols  
(248) 594-6360  
cnichols@plunkettcooney.com



Jason G. Bulbuk  
(248) 594-2879  
jbulbuk@plunkettcooney.com

**BYOD 2.0** **PLUNKETT COONEY**  
ATTORNEYS & COUNSELORS AT LAW

---

---

---

---

---

---

---

---

**Presentation Preview**

- BYOD: Where are we at today?
- BYOD Risks
  - Security, Privacy Wage and Hour
- BYOD Policy Dos and Don'ts
- BYOD Litigation Issues

**BYOD 2.0** **PLUNKETT COONEY**  
ATTORNEYS & COUNSELORS AT LAW

---

---

---

---

---

---

---

---

## What is BYOD?

Use of employee-owned mobile devices such as smartphones and tablets to access business enterprise content or networks.



BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Recent BYOD Developments

- “BYOD trend” began approximately five years ago.
- Initial estimates:
  - Four in 10 organizations will rely exclusively on BYOD by 2016 and 85 percent will have some kind of BYOD program in place by 2020.

*Continued*

BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Recent BYOD Developments

- Recent trend:
  - Less businesses using BYOD
  - Survey in April/May, 2015 – 53 percent of various American businesses allowed **no** BYOD (up from 34 percent in 2013)
    - 7 percent allow a full BYOD policy
    - 40 percent partial policy

BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

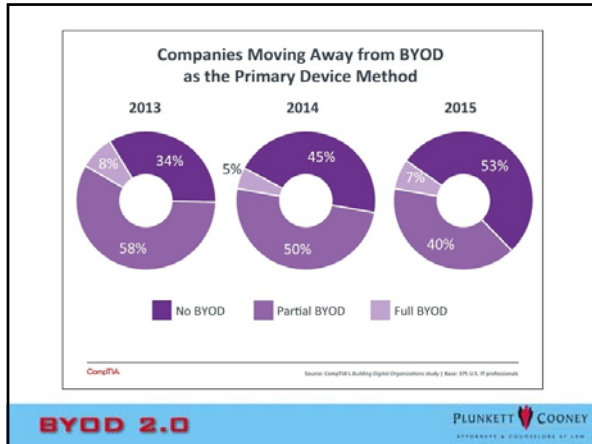
---

---

---

---

---



---

---

---

---

---

---

---

---

- ### Factors Leading Trend Away from BYOD
- “Cloud”
    - Employees not concerned about losing private data upon termination
  - Belief that risks may outweigh benefits
  - Adverse business climate for BYOD in Europe
    - Complex regulation, tax regime, high mobile data cost
    - Results in many employers providing devices in European countries
- BYOD 2.0 PLUNKETT COONEY ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

- ### What are the Risks?
- Data security breaches
  - Invasion of employee privacy
  - Wage and hour violations
- 
- BYOD 2.0 PLUNKETT COONEY ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Security Issues

- Major Issue: Enforceability of security policies
  - According to research conducted by Gartner, one in four business users surveyed had a security issue on their private device.
  - According to Osterman Research, 15 percent of employees believe they have “none to minimal” responsibility to protect corporate data stored on their personal device.

BYOD 2.0



---

---

---

---

---

---

---

---

## How to Limit Security Breaches

- Require data encryption, password protection, automatic log-out, automatic lock-down and remote wipe capability.
- Have users install a “sand box” on a personal mobile device.
  - Consists of a password-protected encryption and holds only business’ files and information.

BYOD 2.0



---

---

---

---

---

---

---

---

## How to Limit Data Security Problems

- Implement external, offsite backup system for user data based on data classification and sensitivity.
- Network security: network-enforced password that should be rotated on periodic basis
  - Minimum password lengths, special characters, etc.
- Educate employees with access to confidential data.
  - If you call data confidential but did not tell anybody it is confidential, it is not *really* confidential.
  - Training on policies

BYOD 2.0



---

---

---

---

---

---

---

---

## How to Limit Security Breaches

- Healthcare Industry:
  - National Institute of Standards and Technology's National Cybersecurity Center of Excellence released a draft guide for healthcare providers on mobile device security.
  - Step-by-step guide:
    - [https://nccoe.nist.gov/projects/use\\_cases/health\\_it/ehr\\_on\\_mobile\\_devices](https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices)



BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Privacy Issues

- Biggest concern employees have:
  - MobileIron Trust Gab Survey: 70 percent of employees don't trust their employer with personal data.
- Monitoring employees on/off company time and premises
  - Example: requirement that location services be turned on
    - Employer can track employee
    - Employees want turned off for personal reasons

BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Computer Fraud & Abuse Act

- Federal CFAA makes it a **criminal offense** to gain unauthorized access to a computer and permits recovery of civil damages when authorized access results in damage exceeding \$5,000.
- All 50 states have enacted "computer trespass" laws, which largely parallel CFAA.



BYOD 2.0

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Stored Communications Act

- Criminal statute with civil remedies
- Prohibits unauthorized access to email stored at an email service provider

*Continued*

**BYOD 2.0**

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Stored Communications Act

- Example:
  - *Pure Power Boot Camp, Inc. v Warrior Fitness Boot Camp, LLC.*
    - Employer accessed former employee's Hotmail account using log-in credentials stored on employer's computer system.
    - In Hotmail account, found log-in information for Gmail account and accessed information in that account as well.
    - Former employee obtained summary judgment in his favor.

**BYOD 2.0**

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

## Recent Case Law Guidance

- *Rajae v Design Tech Homes, et. al.* (TX)
  - Company remotely wiped sales representative's iPhone when he resigned.
  - Deleted all data, personal and work-related
  - Ex-employee sued under SCA and CFAA.

*Continued*

**BYOD 2.0**

PLUNKETT COONEY  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

### Recent Case Law Guidance

- Court rejected both claims.
  - Information in cell phone is not “electronic storage” under ECPA.
  - Was not a CFAA-qualified “loss” even though he lost all of his personal photos, videos, contacts and passwords

BYOD 2.0




---

---

---

---

---

---

---

---

### Case Law Guidance

- *Quon v City of Ontario*
  - Issue: whether employee had a reasonable expectation of privacy for private messages sent and received on city-owned device while off duty and whether search of that data was reasonable
  - Ruling: policies in place governed employee’s rights to the extent those stated policies were enforced.



BYOD 2.0




---

---

---

---

---

---

---

---

### Wage & Hour Issues

- Off the Clock Work
  - If nonexempt employee uses his/her mobile device to conduct work-related business → risk that employee will raise wage and hour claim for “off the clock” work.
  - Even if use is voluntary and without directive from employer, employee must be compensated for time spent making work-related calls or reading and writing emails.

*Continued*

BYOD 2.0




---

---

---

---

---

---

---

---

### Wage & Hour Issues

- Remember: both FLSA and Michigan’s Minimum Wage Law require that all nonexempt employees be paid for all time work, including overtime.
- This includes all time that employees are “suffered or permitted” to perform work.

BYOD 2.0



---

---

---

---

---

---

---

---

### Wage & Hour Issues

- Expense Reimbursement
  - FLSA prevents employers from requiring employee to pay for business expenses of employer if doing so reduces employee’s earnings below required minimum wage or overtime compensation.
  - Eleven states have express or implied statutory expense reimbursement requirements.
  - Michigan: MCL 408.477(1)

*Continued*

BYOD 2.0



---

---

---

---

---

---

---

---

### Wage & Hour Issues

- Except for those deductions required or expressly permitted by law or by collective bargaining agreement, employer shall not deduct from wages of employee, directly or indirectly, any amount including employee contribution to a separate segregated fund established by a corporation or labor organization under section 55 of Michigan Campaign Finance Act, 1976 PA 388, MCL 169.255, without full, free and written consent of employee, obtained without intimidation or fear of discharge for refusal to permit the deduction.

BYOD 2.0



---

---

---

---

---

---

---

---



### How to Limit Wage & Hour Issues

- Train supervisors to identify off-the-clock work and to **not** reinforce that behavior.
- Potentially implement a policy requiring prior written authorization to work remotely via mobile device.
  - Instruct employees that, unless authorized, all emails should be responded to only during working hours.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### How to Limit Wage & Hour Issues

- Revise leave of absence policies to remind employees that they are not to be performing work during a leave of absence
  - Deactivate employee's connection to company's data and systems and/or reconfigure system so calls/emails are redirected to another address.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### How to Limit Wage & Hour Issues

- Decide reimbursement method that best fits your company: reimburse payment of actual expenses or issue lump sum payment estimated to fully compensate employees.
- Require employees to track and report **all** time work, including any time spent on personal devices after hours.
  - Can specifically include in policy a requirement that employees record time spent responding to emails and answering phone calls while out of office

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Recent Case Law Guidance

- *White v Baptist Memorial Health Care Corp.* (6th Cir.)
  - Employer awarded summary judgment because plaintiff failed to report time in exception logs
    - If employer establishes reasonable process for employee to report uncompensated work time, employer is not liable for non-payment if employee fails to follow the established process.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Recent Case Law Guidance

- *Mohammadi v Nwabuisi* (TX)
  - Employer found liable for not compensating employee for overtime work performed on employee-owned device

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Curing the BYOD Hangover

- BYOD Hangover: reaction to changing nature of BYOD and inherent risks
- Technical solutions
  - Used by analysts, writers and members of mobile industry
- Policy language

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Technical Solutions to BYOD Concerns

- Implement technical controls
  - **Sandbox**
  - Mobile Device Management (“MDM”) software
    - Require encryption of data stored on device.



*Continued*

**BYOD 2.0**

PLUNKETT & COONEY  
ATTORNEYS AT LAW

---

---

---

---

---

---

---

---

### Technical Solutions to BYOD Concerns

- Require strong passwords for access.
- Force wipe of device after 10 unsuccessful password attempts.



**BYOD 2.0**

PLUNKETT & COONEY  
ATTORNEYS AT LAW

---

---

---

---

---

---

---

---

### More Technical Solutions...

- Enterprise Mobility Management
  - IT solution
  - Offered by different vendors
    - i.e., Dell AirWatch®
  - Generally: controls complete mobile device
  - Can provide separation of corporate and personal data



**BYOD 2.0**

PLUNKETT & COONEY  
ATTORNEYS AT LAW

---

---

---

---

---

---

---

---

### Review of Solutions & Appropriate Policy Language

- Modify current policies → *all policies apply when using BYOD device.*
  - Harassment, discrimination and EEO policies
  - Time recording and overtime
  - Acceptable use of technology
  - Data privacy and security
  - Confidentiality and trade secret protection

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Policy Dos

- Employees may have opportunity to use their personal electronic devices, including personally-owned cell phones, tablets, laptops and computers, for work purposes after receiving written authorization.
- Use of personal devices is limited to certain employees and may be limited based on technology.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Policy Dos

- No employee should have any expectation of privacy except that which is governed by law.
  - Company may monitor and preserve communications that utilize company's networks in any fashion, including data, voicemail, telephone logs, internet use and network traffic, to determine proper utilization.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Policy Dos

---

- Employees are expected to protect personal electronic devices used for work-related purposes from damage, loss or theft. Thus, employees are required to have remote-wipe software installed on their personal electronic devices (that are used for work-related purposes) by the IT department prior to use, and employees must notify management immediately if their personal electronic device is lost or stolen.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Policy Dos

---

- This software will allow the company to erase company-related data remotely in event the device is lost, stolen or otherwise compromised. Wiping company data may affect other applications and data.
- Company will not be responsible for loss or damage of personal applications or data that results from use of remote-wipe software.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Policy Dos

---

- Upon termination or resignation of employment (or at company's request), employee may be asked to produce his or her personal electronic device (used for work-related purposes) for inspection. All company data on personal electronic devices will be removed by IT upon termination or resignation of employment.
- Failure to follow these policies and procedures may result in disciplinary action up to and including termination of employment.

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Impacts of BYOD in Litigation

- Complicates e-discovery process because electronic data may reside on devices besides those over which company has control.
- Must consider this when enforcing a litigation hold.
- Threshold question: whether a litigant has “possession, custody or control” of information sought.

BYOD 2.0




---

---

---

---

---

---

---

---

### Case Law Guidance

- “Possession, custody, control” = fact specific inquiry
- *Small v Univ. Med. Center of S. Nevada*
  - eDiscovery special master recommended “death penalty” sanctions on defendant for failing to preserve data stored on mobile devices.
  - No litigation hold notice issued re: BYOD devices
  - Lost over two years of messages and other ESI



BYOD 2.0




---

---

---

---

---

---

---

---

### Case Law Guidance

- *Financial Wealth Management v McMullan (CT)*
  - Required defendants to submit personal computers for imaging because used for company purposes.
- *In re Pradaxa (IL)*
  - Court held that a litigation hold should extend to personal company-issued devices in order to preserve any text messages that might be relevant to the lawsuit
- *Cotton v Costco Wholesale (KS)*
  - A company did not have “possession, custody or control” over text messages sent by its employees.
  - Company did not have the legal right to obtain on demand any text messages on the employees’ personal cell phone.
    - No allegations phones issued by or used for Company purposes.

BYOD 2.0




---

---

---

---

---

---

---

---

### New Trends To Consider

- CYOD
  - Choose Your Own Device
    - Employees offered a suite of choices that company has approved (security, reliability, etc.).
    - Devices work within company IT environment but employees own the device.

*Continued*

**BYOD 2.0**



---

---

---

---

---

---

---

---

### New Trends To Consider

- COPE
  - Company issued, Personally Enabled
    - Employees supplied phone chosen for and paid for by company, but they can also use it for personal activities.
    - Company decides how much choice and freedom employees get.

**BYOD 2.0**



---

---

---

---

---

---

---

---

### Questions?



**BYOD 2.0**



---

---

---

---

---

---

---

---

**Post Webinar Survey Reminder**

**BYOD 2.0** **PLUNKETT COONEY**  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

**Upcoming Webinar – Nov. 19**

**Hot Topics Webinar**

Noon to 1:15 p.m.

**BYOD 2.0** **PLUNKETT COONEY**  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

---

---

---

---

**The Sophisticated Employer**  
Your legal resource for workforce management

**Federal Contractors will be Required to Provide Employees Paid Sick Days**

POSTED BY CLAREDA Q. USIB  
SEPTEMBER 16, 2015

Presidential executive order requires federal contractors entering into contracts after Jan. 1, 2017 to provide their employees with sick days. [Continue Reading](#)

TAGS: HUMAN RESOURCES, LABOR LAW

Comments: 0 Questions to the Author

**PLUNKETT COONEY**  
DETERMINED. DISTINCTIVE. FEARLESS.<sup>SM</sup>

Subscribe Via: RSS, EMAIL

**BYOD 2.0** **PLUNKETT COONEY**  
ATTORNEYS & SUGGESTIONS AT LAW

---

---

---

---

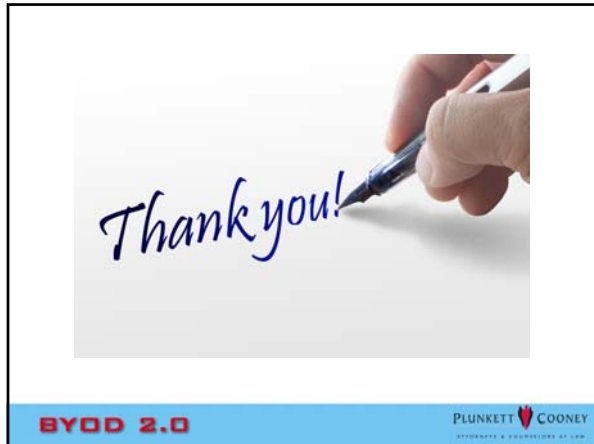
---

---

---

---





---

---

---

---

---

---

---

---