Bring Your Own Device To Work (BYOD) Risky Business???
What is BYOD

- Bring Your Own Device
- Rapid increase in the use of mobile devices by employees
  - iPhones, iPads, Android devices, etc.
- Employees utilize these devices to perform work for you
  - Whether company provided or employee’s personal device
- Result: “Dual-Use” Device
  - Both personal and company data and activity
  - Handling personal matters while at work – more difficult to monitor
- Why allow it? You may not have a choice
Advantages - Company

- Expected in today’s fast paced and instant gratification environment
  - Tablets and Smartphones are replacing traditional PCs & laptops

- Cost savings
  - Is it really? Security; Reimbursement, Internal Service, & Risk of lost devices
    - Less bargaining power in cellular and data plans

- Improves Employee Productivity and Availability
  - Always reachable, employees are familiar with device functions and capabilities
Advantages - Employees

Mobility
  - Work remotely: Home and on the road

Work/Life Balance
  - Good Technology Survey:
    - 76% of enterprises support BYOD
    - 80% of people continue working when leave the office
    - 7 extra hours/week = 365 hours/year
    - 50% check work email in bed
    - 38% at dinner table
    - 57% on family outings

Personalization/Familiarity
  - Employees know their devices

Choice
  - Eliminate the need for two devices
  - Allow employees to choose own device
Risks & Challenges

- **Upgrades:** Too fast for Company to keep up
- **Data stored on mobile/personal devices not owned by the Company**
  - Corporate information and trade secrets
  - Personal information of employees and/or customers
- **Mixing of personal and corporate data**
- **Malicious Software Attacks**
- **Compliance risks**
  - HIPAA
  - Encryption (MA & NV)
  - Client demands
  - eDiscovery
Additional Security Risks

- **Outside Threats**
  - Unsecured network access
  - Lost/Stolen Device

- **Family and Friends**
  -- Children/Spouse/Nosy Cousin

- **Public at large**

- **Result = Data Breach**
Data Breach

How can you make sure you don’t experience a breach?
- You can’t!

What is a “data breach”
- An entity knows or has reason to know that personal information (Name + SSN/FIA/State ID/DLN/Biometric/Medical) of one or more individuals was acquired or accessed by an unauthorized person
- 46 States + Federal Law (e.g. HIPAA)

Devices may contain all of this
- The lost device; Inadvertent access; Theft/intentional acts; Inadvertent email attachment/forward/”reply all”—easy on BYOD; Remote access/Wireless networks

Handling the breach (notice—Individual/State Agencies, public relations, etc.)
Who Is Affected By A BYOD Program

- Legal
- Human Resources
- Finance
- Communication/Employee Relations
- Information Technology
Legal Issues

E-Discovery Obligations
- Preserving data in connection with litigations

Privacy Laws/Concerns
- Different Throughout the world
  - EU Most Restrictive
- Adapt for locations/countries
- Encryption
- Do you need to get possession of device
- Storage card
- Handling old devices - destruction
- Lowering expectation of privacy
Employee Privacy Concerns with BYOD Programs

- **The Remote Wipe**
- **Accessing truly “personal” information/content**
  - Multiple email accounts
  - GINA/Disability Information
  - Need to access device to update software; monitor up to date
- **Privileged Communications**
  - *Stengart* (N.J. Supreme Court)
Legal Issues

Additional Risks Beyond Privacy

- **Safety**
  - Mobile Device use and driving

- **Unions**

- **Employee Conduct**
  - Negligent Hiring/Supervision
  - Discrimination, Harassment, Retaliation
Employee Conduct

Negligent Hiring/Supervision

An employer may be held liable for an employee’s wrongful acts if the employer knew or had reason to know of the risk the employment created.

- **Doe v. XYC Corp.**, N.J. Super. 122 (2005) (Court found employer liable as it had duty to investigate and respond in case of alleged negligent supervision of employee who was criminally charged with child pornography using workplace computer).
Legal Issues

Employee Conduct

Discrimination, Harassment and Retaliation

- Employer viewing of conduct may trigger protections of anti-discrimination laws.
  - Continental
- Device may contain information regarding disabilities, sexual orientation, religion and other protected characteristics (Genetic or Medical Information).
- Difficult for employer to prove it did not rely upon personal information.
Legal Issues

Additional Risks Beyond Privacy

- Wage and Hour Issues
  - Tracking employee work time
  - Good Technology Survey
Compensable Time

What is compensable time?

- All work that is “suffered or permitted to work”

- Work is compensable if the employer has any way to know that work was performed, even if not authorized in advance

- Exceptions – *de minimis* work

- Recording time worked
“On-call” Time

General rule – time spent waiting while on-call is not working time (or compensable) if employee is free to use time as he/she pleases

- Determination of whether time is spent “predominantly for employer’s benefit” requires fact-specific, case-by-case analysis
- Consider:
  - terms of employment agreement
  - any physical restrictions
  - response time
  - frequency of actual calls during on call period
  - percentage of calls expected to be answered during on call period
  - how does the employee actually use the on call time
  - disciplinary action imposed on employee who fails to answer calls
Legal Issues

Calculation Considerations

- On-call compensation calculation issues – include in “regular rate” of pay?
  - consider effect on overtime calculations

- On-call pay is to be included in regular rate of pay per DOL regulations and opinion letters
“Email Curfew”

- Concept is to draft a policy that prohibits nonexempt employees from emailing when off duty.
- Tension between business need for instant access and paying employees to be responsive to client/customer needs.
- Training of managers and Company expectations.
Procedures
- Hiring
  - Notification of program and executed agreement
  - How to get “hooked up” to the program
- Cessation of Employment/Change of Position
  - Device will not be returned
    - Removing Data

Access Restrictions
- Employees v. Management
- Cannot restrict personal usage
Human Resources Issues

- All company policies apply
  - Update existing policies
    - Electronic communications, Social Media, Harassment/Discrimination

- Training – Education/Responsibility

- Reimbursement/Cost Sharing

- Monitoring
  - How and by whom (need to consider limiting)

- Coordinate breach response (IT, Legal)
Reimbursement/Cost Sharing

- Voice/Data plan
  - What types of plan?
- Device
- Maintenance/Repair
How is this program explained to management?
- Everyone on-board

How is this program explained to employees?
- The “sell”
- Support from HR and IT
BYOD IT Issues

Accessibility vs Security
Accessibility vs Security

- Inverse relationship
- Can’t have it all
- Find the sweat spot for your organization
Factors at Play

**Accessibility (Users)**
- Latest hardware
- Just get it done attitude
- Control (My Device)

**Security (IT)**
- Management and Support
- Compliance (Data Breach)
- Control (Our Services)
Matter of Perspective

- Small Business
- Medium Business
- Large Business
- Highly Regulated Industries
Management and Support

- Restrict supported devices?
- What level of support do you provide?
- Device Security/Compliance Audits?
- Mobile Device Management (MDM) system?
IT Issues

Security

- Encryption?
- Screen Locks
  - Pin, pattern, alpha-numeric?
  - Wipe on Failure?
- App restrictions?
- Remote Wipe?
  - Implications
  - Selective Wipe
Data Breach Risks

- Human Factor
  - Will users tell you about lost/stolen/damaged devices first?
  - Malware
  - Selling or giving away of device
  - Removing data when an employee leaves
Prepare

- Have a Comprehensive Employee Exit Strategy

- Lost devices will happen!

- Written policies should be clear, communicated, and employees trained

- Test your plan and enforce it
Dealing with BYOD
Key Elements of BYOD Policies

**Eligibility**
- Eligibility Requirements
- Device support limitations
- Risk and responsibilities
- Access limitations
  - Role/Title/Geography
- Applicability of other policies
Reimbursement

- Conditions for reimbursement
  - Device purchase and/or replacement
  - Plans
  - Limitations (e.g. max amount)
  - Substantiation of expenses
Dealing with BYOD
Key Elements of BYOD Policies

End-User (employee) Support

- Define what devices are supported
- Define types of support provided
  - Applications, services, scenarios
  - “Self-service”
- How to request support
Dealing with BYOD
Key Elements of BYOD Policies

**Security**

- Prohibit
  - “Jail Breaking” or “Rooting”
  - Modifications to device hardware or operating software beyond routine updates
- Process and timing for reporting loss, theft, new device, unauthorized access, and cessation of employment
  - Remote Wipe
- Password and/or encryption requirements
  - Encryption required?
  - Failed Login
Dealing with BYOD

Key Elements of BYOD Policies

- **Data**
  - Classify devices, users and data accessed
  - Clarify ownership of Apps and Data
  - Establish Allowable Apps and Banned Apps
  - Employee Exit Procedure
Dealing with BYOD
Key Elements of BYOD Policies

- **Monitoring**
  - Balance the expectations of privacy
    - Reserve right to monitor
    - Voluntary acceptance of program
    - Explicit Consent in writing
    - Postings? (Walls, Login Screen, Homepage)
  - **Quon** (9th Circuit – Appealed to U.S. Supreme Court)
    - Be consistent in content and application of policies
Policy Violations

- Clear on consequences
  - “Up to and including termination”
- May need to notify business partners
Additional Key Elements of BYOD Policies

- Guidelines on device configuration
- Safety (e.g. vehicle use)
- Plan for breach
- Develop process for litigation preservation, data deletion, device and security updates
- Training
Take Aways

- Be Prepared
- Don’t Be Left Without A Good Story To Tell
- Monitor Legal Developments

Visit our blog: [http://www.workplaceprivacyreport.com](http://www.workplaceprivacyreport.com)
QUESTIONS?