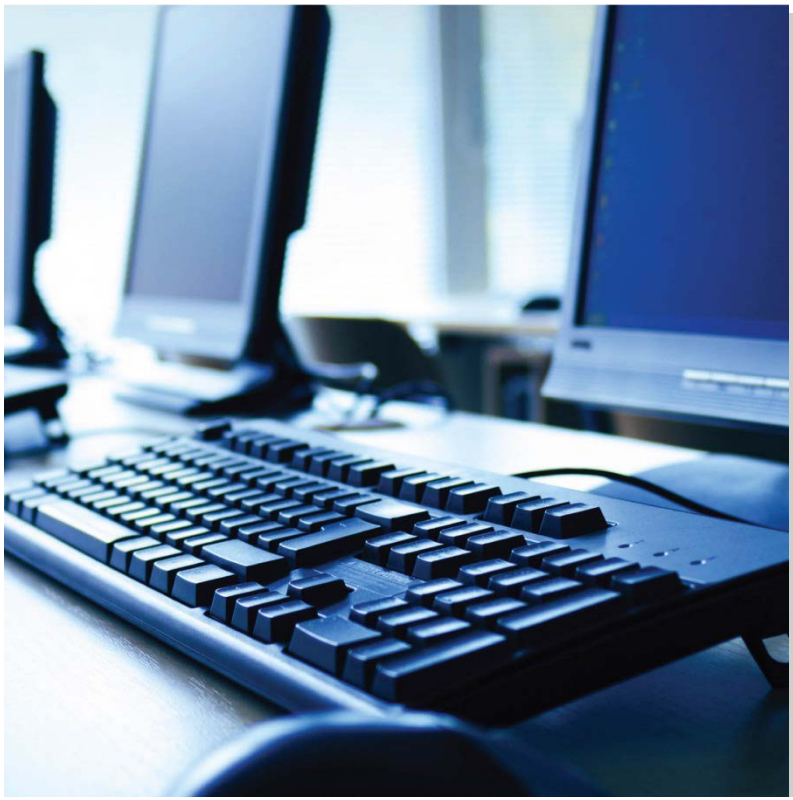
Ballard Spahr LLP

Avoiding the Pitfalls of 'Bring Your Own Device' Policies



BYOD/T Represents a Constant Battle Between Compliance Objectives and Employee Usability

Presenters:

Constantinos "Dino" G. Panagopoulos, Labor and Employment Group

Philip N. Yannella, E-Discovery and Data Management Group

Amy S. Mushahwar, Privacy and Data Security Group

June 12, 2013

Agenda

- Background:
  - Options, Options Everywhere..
  - Technical Solutions
  - Legal Background
- Specific Legal Issues
  - Intellectual Property
  - Privacy / Security
  - eDiscovery
  - Employee Investigation Risks
- Risk Management Program
- Topical Checklist

Background

Background

- What's this mobile alphabet soup?
  - MDM?
  - BYOD?
  - BYOT?
  - SOYD?
  - SOYT?

Background

- Employees have an expectation of personal privacy on their devices and on loosely managed devices.
- Consider all of the following uses (that now could contain company communications, cloak company communications or confer legal liability):
  - Personal phone calls,
  - Personal texts,
  - Personal app usage,
  - Cloud storage provider use (iCloud/Box),
  - Personal content downloads
- Given the ongoing intermingling of personal and professional communications, active policy management is key!

Options, Options Everywhere

From Most to Least Corporate-Controlled

1. Corporate-owned stringently managed devices
2. Corporate-owned loosely managed devices
3. Devices purchased by employees with an employer device or service subsidy.
4. Devices purchased by employees that will access the Corporate network

Technical Solutions

- Containerization
- Enterprise Solutions
- Phone Segmentation

Good™

airwatch™
mobile device management

CITRIX®
ZENPRISE

Legal Background: What Is the Stored Communications Act (SCA)?

- 1986 Act, passed as part of the Electronic Communications Privacy Act (ECPA)
- Generally speaking, SCA protects "stored communications"
- Legislative history of SCA
  - Passed at the dawn of the Internet Age
  - Concern over scope of 4th Amendment protection for internet-enabled communications

Legal Background: What Does SCA Protect?

- SCA prohibits intentional and unauthorized access to a ***facility*** through which an ***electronic communication service*** operates
- Prohibits any person or entity from obtaining, altering, or preventing access to electronic communications in ***electronic storage.***

Legal Background: What Does SCA Protect? (cont'd)

- "Facility" Not Defined
- "Electronic Communication Service" is:
  - "[A]ny service which provides to users thereof the ability to send or receive wire or electronic communications."
- "Electronic Storage"
  - Temporary, intermediate storage of electronic communication or storage for purposes of back-up protection

Legal Background: SCA Scope and Penalties

- Criminal and civil penalties
- Compensatory and punitive damages potentially available
  - Statutory damages – minimum of $1000.
  - Punitives available absent actual damages

Legal Background: What Accounts are Protected?

- Internet Email
- Non-public Facebook accounts
- Remote cloud-based services

Legal Background: What Is Not Protected Under SCA?

- Public Information
  - Twitter feeds
  - Public portions of Facebook
- Metadata (date sent, account holder, country of origin)
  - Covers content only
- Private Communication Services
  - Work email, *e.g.*
- Data Stored Locally

Ballard Spahr LLP

Legal Background: The Problem of BYOD/T

- Dual-use policies that permits use of personal devices for work purposes
- Company policies may cover access to company-provided accounts **but don't necessarily** cover personal accounts
- Employers may be unaware that they don't have unfettered rights to access materials on a dual-purpose device

Specific Legal Headaches

Ballard Spahr LLP

Intellectual Property Concerns

- **Catch-22**: more device control may be a security good but it may create additional IP liability. Weigh this risk with your legal counsel.
- Corporate liability for infringement/ contributory infringement (delicate dance between audit control vs. willful blindness)

Privacy and Security Risks

- Know your privacy and security obligations under applicable laws
- Relevant applicable laws may include:
  - Federal sector-specific statutes (FERPA, HIPAA, GLB, etc.)
  - Generally applicable state data security laws requiring everything from "reasonable security" to more specific safeguards, most notably Massachusetts' new data security regulations
  - State encryption laws
  - State breach notification laws
  - Social security number privacy laws
  - Evidence and e-discovery obligations

BYOT-Security Concerns

- E-mail may be cut and pasted to a non-secure location off of the company e-mail server
- Business documents may be opened outside of the secure location off of the company e-mail server
- Devices could become infected with mobile malware, enabling hacker to obtain confidential data

Security Tension

Happy Medium:

-Reasonable compliance
-Confident but not over doing it

Too Much Security:

-Employees will circumvent compliance settings

-Difficult to maintain

Too Little Security:

-Data will not be protected
-Free-for-all

eDiscovery

- Comingling of personal and business data on a device poses big problems
  - Employees may be doing business over protected personal accounts
  - Forensics may reveal passwords to SCA-protected accounts
  - Forensics may reveal data that you do not want to know in the context of litigation

eDiscovery and MDM

- If litigation has ensued, personal email and social media accounts may need to be preserved
- Litigation hold should ask employees to take appropriate steps to preserve relevant data in such accounts

BUT

- **Company does not have legal control of personal accounts and cannot preserve or collect data from such accounts absent employee consent.**

Employee MDM Risks: Best Practices For Internal Investigations

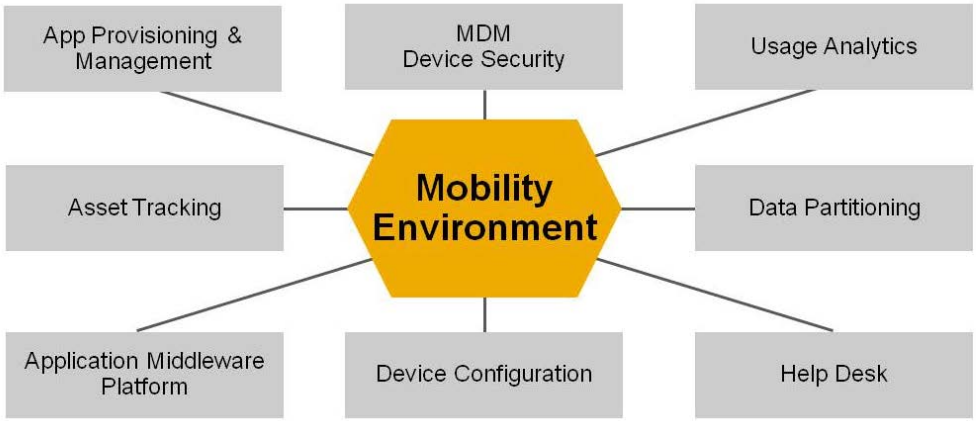
- Interview employee
  - Identify types of communication services used on device
- If there are protected accounts on personal device used for work that you think you need to access
  - Get written consent
  - Trend is to construe BYOD policies narrowly in favor of privacy rights

Best Practices for Employee Investigations (cont'd.)

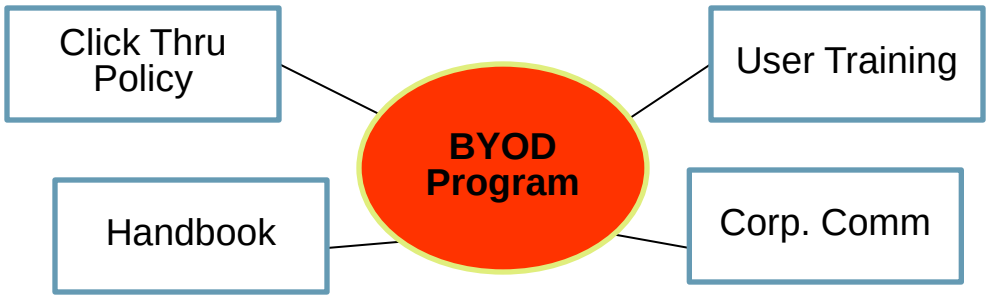
- If there are protected accounts on work-provided devices
  - Do not assume you have right to access such accounts
  - Determine whether you have need to access such accounts and if so, get consent
- Talk to forensic vendors to ensure that no one accesses protected accounts

Addressing the “Issues” via Risk and Operational Management

Technical



Legal



Ballard Spahr LLP

Employee MDM Program

- Long form notice in a company handbook may not get noticed by your employees!
- Best practice: Layered notice
  - On device click-through MDM policy,
    - ✓ More than the Apple warning!
    - ✓ Policy should remain accessible to the employee on the device
    - ✓ Let me know if you need samples
  - Handbook notice,
  - Deployed company training and
  - Integrate MDM education statements in existing privacy/security corporate communications.

Topical Issues Checklist for MDM Policy

- Employee Overtime
- Phone Usage While Driving
- MDM Software or Container?
- Device Wiping (all or limited wipe)?
- Level of Audit Control?
- Geolocation?
- Encryption (device, content or virtual environment)?
- Application Purchases (whitelist / blacklist / company store)
- Malware / Viruses (software / hardware scanning Devices)
- Cloud Services
- E-Discovery

Questions?

Amy Mushahwar
202.661.7644
mushahwara@ballardspahr.com

Dino Panagopoulos
202.661.2202
cgp@ballardspahr.com

Phil Yannella
215.864.8180
yannellap@ballardspahr.com

Ballard Spahr LLP