Third Thursday –Crowell & Moring's Labor & Employment Update

June 20, 2013

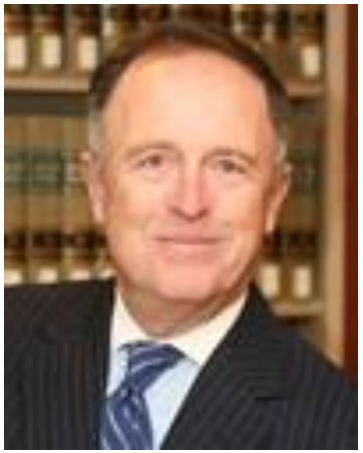
The webinar will begin shortly. Please stand by.

Today's Presenters

Chris Calsyn

Robin Campbell

David Cross



Tom Gies

BYOD – Employment Law Compliance

- Wage Hour Laws
- Traditional Labor Law – Duty to Bargain
- EEO laws
- HIPAA and other Industry-Specific Regulations
- Stored Communications Act
- State-specific privacy laws

BYOD Policy Design – Employment Law/HR Considerations

- Eligible employees
- Permissible use - business and/or personal
- Reimbursement of expenses
- End-user support
- Security Issues
- Limitations of liability for any inadvertent loss of personal information

BYOD – Employee Concerns

- Consent and other consideration issues
- Reservation of employer rights
  - Access
  - Monitoring
  - Confiscation
  - Notice before accessing device

BYOD - Policy Design/Administration

- Company monitoring
- Access to the device
- Lost devices – “remote wiping”
- Investigations of employee misconduct
- GPS monitoring

Legal Data Security Requirements

- HIPAA
- GLBA
- State security mandates
- Data destruction laws
- Global Data Protection laws
- Client contractual requirements

BYOD – Data Security Issues

- System is only as secure as the least secure user/portal device
- Data breaches still largely a result of employee errors (lost devices/misdirected email)
- Notification requirements are broadening (HIPAA) and expanding (EU regulations)

Security Measures

- Identity and access control
- Encryption
- Remote wipe capabilities
- Password protection
- Virus/malware protection
- Security breach notification

Don’t just address in written policies, regulators expect practical training around mandated procedures

BYOD Security Issues

- Risks/security are generally the same as with any portal device—Special BYOD risks:
  - Native encryption does not meet NIST standards
  - Ensure that mobile device management meets legal requirements/business needs
  - Combined viewing of personal and work email—business email can go out under personal
  - Client relation risks (automated signature)
  - Incident reporting

BYOD – E-Discovery Issues

- Company rights
  - Specify accessible data
    - "Practical ability" test
    - Email: company vs. personal
    - Apps: texts, photos, voicemails, call history, contacts, notes, voice memos, calendar, reminders, navigation, web browser, passbook, social media, etc.
  - Notice before access

BYOD – E-Discovery Issues

- Employee duties
  - Prompt access
    - *Southeastern Mechanical Services, Inc. v. Brody*, 2009 WL 2883057 (M.D. Fla. Aug. 31, 2009) – spoliation involving Blackberry® devices
  - Testimony
    - Authentication, chain of custody, foundation
    - Defending discovery process

BYOD – E-Discovery Issues

- Preservation
  - Identify personal devices
  - Identify data sources / apps
    - *Christou v. Beatport, LLC*, 2013 U.S. Dist. LEXIS 9034, 36-39 (D. Colo. Jan. 23, 2013) – spoliation involving iPhone®
  - Identify data storage
    - Mind the cloud
    - Backup / restoration
  - Confiscation

BYOD – E-Discovery Issues

- Collection
  - Self vs. IT vs. Vendor
  - Scope
    - Custodian culling
    - Do not assume data is on company servers
  - Tools
    - Encryption
    - Different vendors may yield different images
  - Format

BYOD – Trade Secret Protection Issues

- Onboarding and BYOD
  - Establish a repeatable process with HR
  - Determine protection strategy
    - Which employees will sign which agreements?
    - What are you trying to protect?
    - How are you trying to protect it?
  - Educate employees about what constitutes trade secrets and protected proprietary information
    - Confidentiality agreements as part of or in addition to BYOD agreement
    - Avoid exposing the company to suits from former employers

BYOD – Trade Secret Protection Issues

- BYOD-device use restrictions – CFAA
  - CFAA can be both a tool to protect competitively sensitive data and a liability for unwary employers
  - Private right of action against person
    - Who knowingly and with intent to defraud
    - Accesses a protected computer without authorization, or exceeds authorized access ….
  - Underscores need to maintain BYOD policy that:
    - Restricts employees' authorized access to and use of company computers, servers, email, and other data archives
    - Obtains authorization from employees to allow employer to access employees' devices as needed without violating the CFAA

BYOD – Trade Secret Protection Issues

- "Reasonable Measures" in a BYOD environment
  - Prevent any remote access to trade secrets?
    - Citrix and other platform alternatives
  - Remote wiping capabilities
  - Password protection / encryption
    - Reminder pop-ups for employees
  - Disabling printing and client-side storage capabilities
  - Security audits
    - Monitoring devices/software to protect most valuable assets

BYOD – Trade Secret Protection Issues

- Offboarding and BYOD
  - Establish a repeatable process with HR
  - Demand return of everything
    - Image BYOD devices prior to departure if possible
    - Conduct remote imaging/wiping of devices as needed
  - Conduct forensic searches of systems before and after departure if possible
    - Complications caused by BYOD devices
  - Affirm obligations under existing agreements
  - Preserve evidence
  - Track former employees through social media and other methods

Contacts

Tom Gies
tgies@crowell.com
202.624.2690

David Cross
dcross@crowell.com
202.624.2774

Chris Calsyn
ccalsyn@crowell.com
202.624.2602

Robin Campbell
rcampbell@crowell.com
202.654.6732