Bring Your Own Device
Security and Privacy Legal Risks
Introduction

Information Law Group, LLP

- National boutique firm with focus on information law
- Experienced, nationally-recognized privacy, technology, media, advertising & information management attorneys
- Clients include: Financial institutions, Fortune 10 multinational corporations, Energy, Media companies, payment processors, retailers, start-ups, non-profits
- Co-Chair American Bar Association’s Information Security Committee
- Certified Information Privacy Professional (IAPP)
- Former in-house lawyer for eBusiness Risk Group of multi-national insurance company based in New York

Chris Paschke

- Experience working in federal and state government
- Background in system management and IT security auditing
- Specialises in IT security management and incident response
- Currently manages IT security for a large Colorado school district.
Road Map

- Introduction
- BYOD Basics
- Information Security and BYOD
- Privacy and BYOD
- Incident Response and Investigation of Personal Devices
- Personal Device Use Policies
BYOD Basics
BYOD Drivers

• Mobile device explosion
  • 76 percent of people have Internet mobile device, and 68 percent have a desktop or laptop (Source: Ad Age)
  • But don’t forget laptops and desktops

• Employee satisfaction
  • Too many devices
  • Consumerization of IT (“COIT”)
  • Generational aspect
BYOD Drivers

- Efficiency/productivity
- Cutting-edge technology
BYOD Drivers -- Perceived Cost-Savings

• Device costs
• Data costs
• IT management costs
• Inefficiencies
• True cost savings?
BYOD Statistics

Mobile Web to Rule by 2015

Source: Morgan Stanley Study / Mashable Tech (http://mashable.com/2010/04/13/mobile-web-stats/)
BYOD Statistics

Source: SANS Mobility/BYOD Security Survey, March 2012
BYOD Statistics

Is BYOD Use Allowed?

- Yes: 61%
- No: 37%
- Don’t Know (2%)

Source: SANS Mobility/BYOD Security Survey, March 2012
BYOD Statistics

Policies Supporting BYOD

- Yes (standalone) 17%
- Yes (added to existing) 24%
- Sort of 26%
- No 31%
- Don’t Know 3%

Source: SANS Mobility/BYOD Security Survey, March 2012
Information Security and BYOD
Addressing BYOD Security Risk Strategy

• Not addressing the risk
• Prohibiting BYOD
• Limiting BYOD (e.g. limited employees; limited data; limited connectivity; limited devices)
• “Traditional” technological security controls
Traditional Security Measures

- Determine and limit the type of devices that can be used
- Implement minimum system requirements and configurations
- Install security-related software to the device
- Encrypt company data on the device
- Apply security patches
- Monitor the use of the device to detect misuse, hacking or malware
- Dictate how the device connects to the company’s network
- Install and update anti-virus software
- Provide support for the device
- Obtain/access the device for purposes of an investigation (because the company owns the device).

INFORMATION LAWGROUP
privacy. security. technology. media. advertising. intellectual property.
Security Challenges

• Mobile nature / lost devices
• Personal use = riskier use
  • More opportunities to pick up virus/get hacked
  • Shared devices
  • Lack of IT / security knowledge sophistication (e.g. configurations, patching, anti-virus)
  • Riskier environments
  • Always in use

• Multiple device-types and operating systems
  • May need to be treated/configured/secured differently
  • May pose different levels of security risk
  • Constant change -- new devices getting popular all the time
Security Challenges

- Jailbroken/modded devices
- Think beyond the device
  - Offsite data transfer (“the Cloud”; auto back-up)
  - Applications
  - Social media access and social engineering/social media hacking
  - Device as portal to entire company network
- Lack of control over device, data and security
Security Challenges
Consistency and Legal Risk

• Reasonable security factors
  • Sensitivity of the personal information,
  • Foreseeability of risks
  • Likelihood of damage
  • Medium and format of the record
  • Potential harm from an incident
  • Cost of preventive measures

• Specific security controls required by law or contract
  • Mass personal information protection law

• Comply with own policies
  • acceptable risk
  • subjective reasonableness
Addressing BYOD Security Risk Strategy

- Acceptable Use Policies (e.g. email, mobile devices, Internet, etc.)
- Security Policies (e.g. mobile, encryption, password, anti-virus)
- Social Media Policy
- Wireless Access Policy
- Remote Access Policy
- Remote Working Policies
- Employee Code of Conduct (or other HR Policies)
- Incident Response Policies
- Privacy policies (or PII Handling Policies)
Addressing BYOD Security Risk Strategy

- Authorization and inventorying process
- Compensating controls
- Encryption
- “Sandboxing”
- Mobile Device Management (“MDM”) software
- Tracking/wiping/bricking
- Personal device use policies
- Training

**Key legally:** being able to explain that despite security being different, level of protection/risk is the same
Privacy and BYOD
Privacy Challenges

• Personal nature of device and expectation of privacy
  • Is prohibited web surfing on a company device allowed on the personal device?
  • Personal data: pictures, videos, personal emails, bank statements, tax returns, social security numbers, chat histories, user names/passwords, medical information

• Mobile nature of the devices
  • Remote working and travel (checking to see if employee is where they are supposed to be)

• The employee “creep out” factor (see e.g. requiring employees to provide Facebook password)
Privacy Challenges – Employee Monitoring

- Monitoring of company-owned devices
- Where monitoring may occur on a personal device:
  - While connected to the network
  - Data in transmission between personal device and network
  - Monitoring of “sandboxed” or company area of mobile device.
  - Monitoring of entire device (e.g. key stroke logger; recording browser history, etc.)
- Data collection about usage may be monitoring (e.g. logging)
- Location, location, location
Privacy Challenges – Investigations

- Investigations (internal, criminal, audits)
- Security breach response – forensic investigations
- Litigation holds
- eDiscovery (searching for, preserving and collecting data)
- Information requests/demands/subpoenas/regulatory investigations

Problem: difficult, impracticable/impossible, harmful to try to limit collection and access to non-company information on/from a personal device
Privacy Challenges – Expectation of Privacy

- **U.S. Supreme Court -- City of Ontario, California v. Quon**
- 4th Amendment – unreasonable search and seizure
- Search concerning personal use of a company device
- Applies to public entity, but instructive to private
- **Was there a reasonable expectation of privacy?**
  - Not ruled upon; assumed by the Court
  - Employee policies are a factor in setting expectation
- **Was the search reasonable?**
  - Work-related purpose existed
  - Scope and intrusiveness of the search was limited
Privacy Challenges – Specific Laws

• Computer Fraud and Abuse Act
  • Unauthorized access/use of computer

• Electronic Communications Privacy Act -- Stored Communications Act

• Computer Trespass
Incident Response and Investigation of Personal Devices
Incident Response and Investigation Challenges

• Loss of control
• Inability to remotely access device
• Obtaining physical possession of a device
• Investigation of employees themselves
• Incident detection (lost devices v. breached devices; actual v. reasonably suspected breach)
Incident Response and Investigation Challenges

- Investigations (internal, criminal, audits, customers)
- Security breach response – forensic investigations
- Litigation holds
- eDiscovery (searching for, preserving and collecting data)
- Information requests/demands/subpoenas/ regulatory investigations (either to company or employee directly)
Incident Response and Investigation Challenges

- Obtaining access to the device and data thereon
  - Physical possession
  - Unlocked/login credentials
  - Unencrypted
- Remote wiping, bricking of a device
- Timing issues
  - Incident detection
  - Litigation holds/spoilation of evidence
Incident Response and Investigation Challenges

• Damage to the device
  • Installation of software may be required
  • Data loss
  • Software corruption
  • Loss of use

• Privacy issues
  • Cooperation issue
  • Ability to tie to business need and limit scope
Personal Device Use Policies
PDUP – Key Considerations

• Relationship to other policies
  • Scope of existing policies
  • Conflicts with existing policies

• Key definitions
  • Personal device
  • Security incident
  • Prohibited information
PDUP – Key Considerations

Privilege v. requirement

Personal device system requirements, configuration and limitations

• Remote connectivity
• Device support
• Software installation
• Expectation of privacy
PDUP – Key Considerations

• **Security requirements**
  • May vary by device
  • No sharing devices
  • Software/configuration requirements

• **Security incident response**
  • Detection
  • Notice
  • Cooperation
  • Investigation
  • Remote wiping
PDUP – Key Considerations

• Investigations
  • Internal, assessments and audits
  • Subpoenas
  • e-Discovery/Litigation holds
• Damage and Liability
• Consent and waiver
Q&A
Thank You!

David Navetta, Esq., CIPP
InfoLawGroup LLP
303.325.3528
dnavetta@infolawgroup.com
www.infolawgroup.com