BAKER & McKENZIE

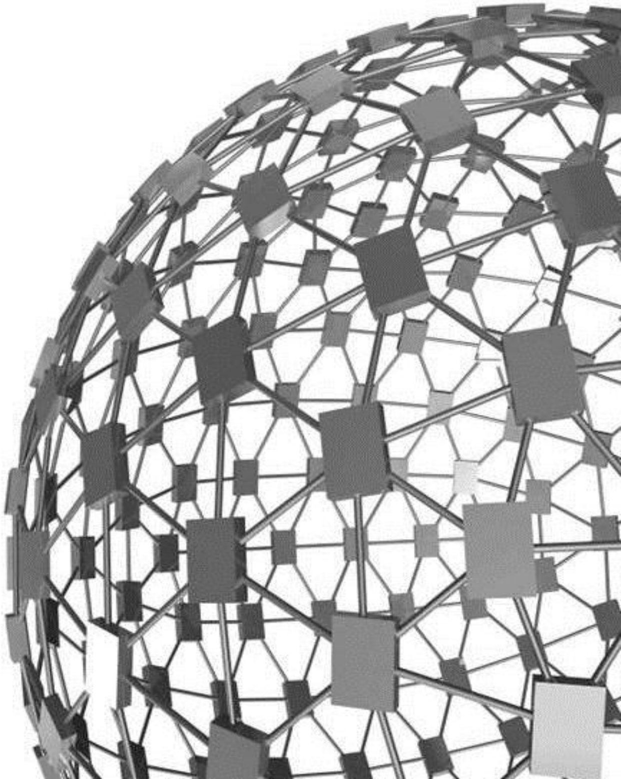
Securing Information Assets in an Insecure Mobile World

May 15, 2012

Brian Hengesbaugh

Baker & McKenzie (Chicago)

brian.hengesbaugh@bakermckenzie.com



Agenda

- Key factual differences when user-owned mobile devices attach to corporate networks
- Key security, privacy, and other legal challenges
- Strategies to manage legal risks
- Take aways

Key factual differences

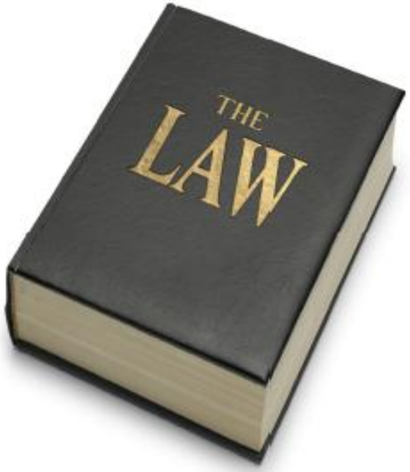
Key factual differences

- Device is not company-owned
- Company might not establish nor maintain security settings on the device
- Company might not be exclusive provider of support services (e.g., third party access to data and device)
- Company may have less control over data (e.g., user uploads to cloud providers and other apps, and user may allow family or others to use the device)
- Employee privacy interests heightened by substantial personal information and user-owned data
- Company may unintentionally invite users to bring highly personal (and perhaps harassing) content into the workplace

Key legal challenges

Key legal challenges

- **Data security and breach notification***
- Legal demands
  - Litigation holds and e-discovery
  - Internal investigations and government demands
- Record retention
- Trade secrets and intellectual property protections
- Harassment and employee claims
- **Computer crimes and user privacy interests***



Data security and breach notification

- Affirmative state data security laws (e.g., Massachusetts)
- State breach notification laws
- Privacy and related tort actions
- Consumer protection laws
- Industry-specific privacy regulations
- Contractual obligations
- Industry standards (e.g., PCI)
- Global (non-US) data security requirements

Computer crimes and user privacy interests

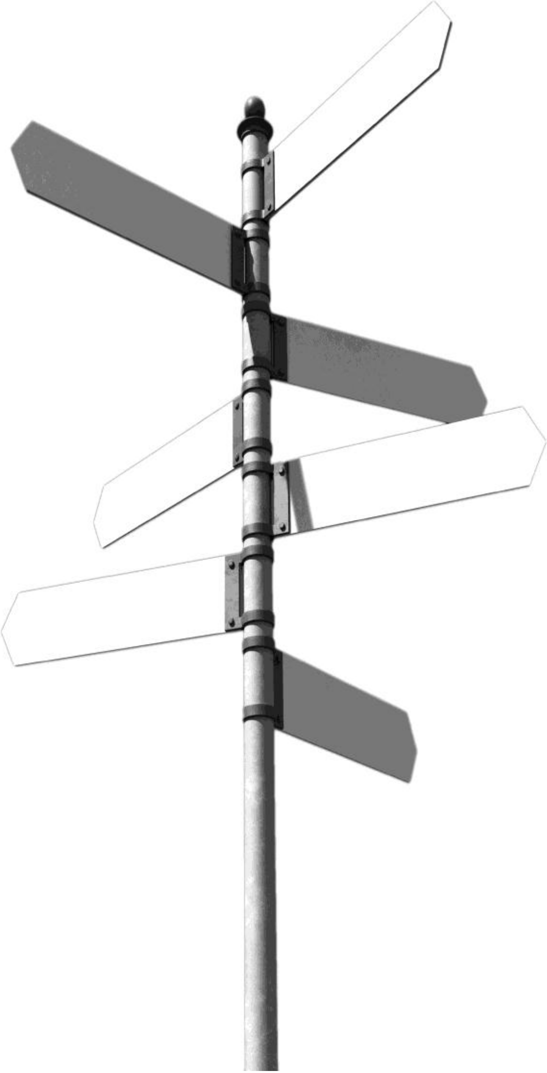
- – Computer Fraud and Abuse Act, and exceeding authorized access*
- – Electronic Communications Privacy Act/ Wiretap Act*
- – Stored Communications Act*
- – State equivalents*
- – Privacy torts
- – Global (non-US) data protection and privacy laws*

NOTE that a "" denotes potential criminal penalties for non-compliance*

Strategies to manage risks

Strategies to manage risks

- **“Big picture” options**
  1. Allow company-owned mobile devices only
  2. Allow user-owned devices to connect to company networks, but entirely prohibit any downloads of company data
  3. Only allow company applications in secure container/sandbox on user-owned devices
  4. Adopt layered approach with different solutions for different user groups and company applications
- **Plus, appropriate policies and procedures (next slide)**



Policies and procedures

- Limit company systems that can be accessed via user-owned devices (risk-based approach)
- Apply all existing company policies to user-owned devices
- Obtain express consent to clear, conspicuous, and comprehensive privacy terms; if drafted properly, should “surprise” users and include provisions such as:
  - Remote access and/or wiping of all content
  - Prohibit upload of company data to “cloud” and third party storage
  - Require immediate notification of lost or stolen device
  - Require production of asset if e-discovery or legitimate demand
  - Require notification before third party servicing of device
- Push security policies that users cannot override (e.g., password complexity, auto wipe after X unsuccessful log-in attempts)
- Support user-owned devices via company security
- Confirm feasibility of security and monitoring policies and procedures in light of employee privacy interests and rights
- Establish internal guidelines for security and other managers on searching and managing user-owned devices

Take Aways

Take Aways

1. Employee-owned devices pose unique legal risks
2. Risk-based analysis of company applications required (e.g., some highly sensitive applications may not be suitable for access via user-owned assets)
3. Solutions to legal issues for company applications require balancing of: (i) data security and other obligations to protect company data against (ii) user privacy interests.
4. Solutions can be “layered” for different user groups and company systems
5. Apply company policies and procedures to user-owned devices
6. Obtain clear, conspicuous, and comprehensive user consents
7. Conduct meaningful training and ongoing review given ever-changing legal standards and security risks

Brian Hengesbaugh

Partner, Baker & McKenzie, Chicago, IL

brian.hengesbaugh@bakermckenzie.com

(312) 861-3077