BYOD At Your Own Risk

Working in the BYOD Era

Shane Swilley
swilley@cosgravelaw.com
(503)276-6074

COSGRAVE VERGEER KESTER LLP
Attorneys

Remember when mobile technology was more Hollywood fantasy than reality …

The original "Smart" Phone

By the 1980s, mobile technology was becoming more accessible …

And, by the early 2000s, cell phones were EVERYWHERE …

Now, employee owned laptops, smartphones & tablets are used regularly for work purposes …

The BYOD Era.

What is BYOD?

BRING YOUR OWN DEVICE

BYOD IS POPULAR … AND GROWING

38%

of US CIOs were expected to support "BYOD" by the end of 2012

82%

of surveyed companies in 2013 allow some or all workers to use employee-owned devices.

Advantages Of BYOD

- Employee can select the devices, software, services and apps they want to use when they want to use them.
- Allows employers to upgrade technology at a quicker rate than budgeting may allow.
- Employees may be more productive/satisfied using devices and platforms they like.
- May be able to shift some or all of costs of device and/or service to employee.

BYOD Alternatives

- **COPE and CYOD models:**
  - Easier for IT to monitor, manage and protect devices because they're employer-owned.
  - Can balance employee preferences with IT resources. Employees can still select devices, services and apps they want to use, but within IT parameters.
  - IT can dictate access to devices to install management software, apply patches, etc. more easily.
  - May allow employer to negotiate service contracts, pool minutes, buy devices in bulk and reap other cost-saving benefits.

Challenges in Managing:

- **SECURITY RISKS**
- **PRIVACY CONCERNS**
- **LITIGATION RISKS**

Security Risks

- **Data leaks**
- **Lost or stolen devices**
- **Unauthorized device sharing**
- **Network Vulnerabilities**

Network Vulnerabilities

- **Devices connected to the network with inadequate antivirus protection**
- **WiFi enabled device create an unsecure "back door" to your network**
- **Installing unvetted apps, hardware or software**
- **Employees who "click first and worry later"**
- **Accessing unauthorized or unsecured networks**

Network Vulnerabilities

Public Clouds and Unsecured Networks

- Corporate files are routinely shared thru third-party cloud sites like DropBox.
- **67%** of companies don't have a policy re: use of these sites.*
- **80%** haven't trained their employees on proper use of these sites.*

* Source: 7/17/13 Survey from Acronis® and the Ponemon Institute.

Privacy in the BYOD Era

Privacy Considerations with BYOD:

- Company access to ensure security
- Unlawful access (intentional and inadvertent) to employee social media and other electronic communications
  - Stored Communications Act
  - Social Media Protection Laws
- Employee privacy rights - 1st and 4th Amendment
- Protection of Private Information
  - ADA confidentiality
  - Common law claims

Litigation Risks

- Wage & Hour Violations
- Data breaches
- Negligence and injury claims
- E-Harassment
- Discovery Issues

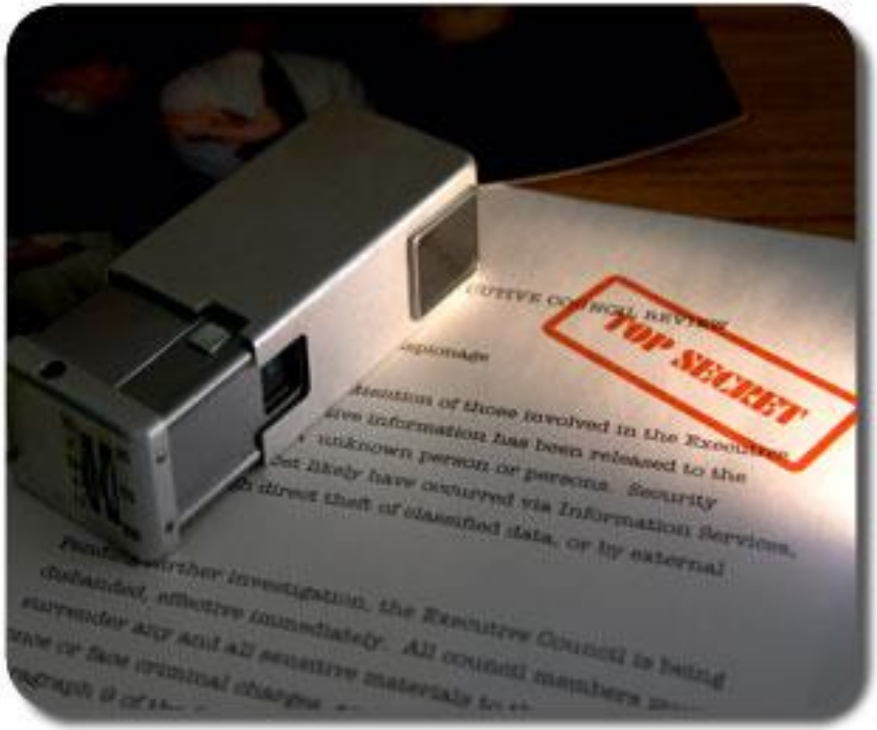
Wage & Hour Violations

80% of people continue working when they have left the office – on average about 7 hours/month or 365 hours/year.*

* Source: based on a survey of 1,000 adults by Good.com.

Data Breaches

- Disclosure of confidential and sensitive information
- Loss of employee personal information



Negligence and Injury Claims

Electronic Harassment

- ***Espinoza v. Orange Co.***, 2012 WL 420149 (Cal Ct App 2012)

  Espinoza worked as a juvenile corrections officer for defendant. Coworkers began posting derogatory and harassing comments about the his disability on a private blog maintained and accessed by employees to discuss work-related issues. Espinoza reported the harassment but defendant did little to stop it. The court of appeals upheld a jury verdict against defendant for failing to prevent harassment.

Electronic Harassment

- ***Guardian Civic League v. Philadelphia Police Dept.*** (2009)

  The Guardian Civic League filed a class-action lawsuit on behalf of 2,300 black police officers against the Philadelphia Police Dept. for not punishing officers who posted racist and offensive content on a website focused on law enforcement.

Other Claims

- Defamation
- False Light
- Public Disclosure of Private Facts
- ADA Duties
- Concerted Activity
- Whistleblower/1st Amendment

E-Discovery

E-Discovery

- **Technology poses some of the biggest discovery and information preservation challenges for the future.**
  - Data created/stored on personal devices such as videos & photos, call logs, voice messages, and GPS information may be discoverable in litigation or as public records.
  - Text messages and other instant messaging tools are increasingly being used for substantive business communications.
  - Tracking, accessing and preserving this information poses logistical and legal issues.
  - This information can also help employers investigate misconduct and defend against legal claims.

What To Do

- **If left unmanaged, employee devices can:**
  - **Lead to a loss of control,**
  - **Impact your network security,**
  - **Cause data loss, and/or**
  - **Result in litigation.**

You need policies that:

1. **Protect both the employer (data/network security & litigation exposure) and the employee (privacy), and**
2. **Define those rights each has regarding use of the devices and the information contained on them.**

Passwords & Key Locks on Devices

- Just **31%** of companies mandate a device password or key lock on personal devices.*

* Source: 7/17/13 Survey from Acronis® and the Ponemon Institute.

Strong Passwords & Key Locks are Critical

You should have a policy for keeping track of passwords for networks and devices

Data Wipe of Lost/Stolen Devices

- Only **21%** of companies perform remote device wipes when employees leave the company or a device is lost, drastically increasing the risk for data leakage.*
- Technology limitations to wiping government data only and preserving personal data.

* Source: 7/17/13 Survey from Acronis® and the Ponemon Institute.

Solution? Limit Device Access

- Look into technology that allows employees to use their own mobile devices to review information, but not allow storage of that government data on the device. If a program is instituted that way, you get away from the legal issues in favor of data security.

Policy Terms

- States employer is not responsible for lost personal data.
- Specifies who owns the device and the information contained on it.
- States employee has no expectation of privacy in government information stored on the device.
- Reserves the employer's right to monitor, search and preserve all government data on the device (within the bounds of the law) and that personal data will not be *intentionally* searched.
- Requires employee to sign and consent to the policy before being allowed to use the device.
- States that employees will be compensated for time worked using the device, even if outside normal working hours.
- Prohibits hourly employees from using the device for work purposes outside normal working hours unless expressly authorized.
- Prohibits the use of the device for work purposes while on unpaid leave unless expressly authorized.

Policy Terms

- If employee pays for device/service; ensures those costs do not reduce employee below minimum wage.
- Prohibits using the device for discrimination, harassment or other policy violations.
- States protocols for passwords and security; accessing networks; disclosing, storing and sharing information; downloading/uploading apps and software; etc.
- States protocols for using (or not using) device while driving or engaging in other risky behavior.
- States protocol for sharing device.
- States the protocols that will be followed when the employment ends.
- Requires the employee to notify management immediately if the device is lost, stolen, damaged, or compromised.
- Dictates who is responsible for fees and costs related to the device.
- Specifies any other prohibited use.

Sample Federal Govt. Privacy Policy

Expectation of Privacy: [AGENCY NAME] will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device) . This differs from policy for government-provided equipment/services, where government employees do not have the right, nor should they have the expectation, of privacy while using government equipment or services. While access to the personal device itself is restricted, [AGENCY NAME] Policy and Rules of Behavior regarding the use/access of government e-mail and other government system/service remains in effect. If there are questions related to compliance with the below security requirements, the user may opt to drop out of the BYOD program versus providing the device to technicians for compliance verification.

The next wave: Wearable Technology

- Google Glass
- Smart Watches/GPS Watches
- Wireless pedometers (Nike Fuel, fitbit, etc.)
- Bluetooth–Enabled Wristbands

And, who knows what new technology is on the horizon?