BYOD (Bring Your Own Device)...
*Liability and Data Breach Sold Separately

December 12, 2013 | Sharon R. Klein, Tracey E. Diamond , Odia Kagan

Pepper Hamilton LLP
Attorneys at Law

We will be starting momentarily…

Pepper Hamilton LLP
Attorneys at Law

Listen to the audio portion of today's webinar by dialing:

North America: +1.866.322.1348

International: +1.706.679.5933

Audio Conference ID: #23512513

Pepper Hamilton LLP
Attorneys at Law

Technical Support Numbers

If you experience technical difficulties, hit *0 on your telephone keypad and an operator will assist you.

Or you can dial:

For Web Support:
+1.877.812.4520 or
+1.706.645.8758

For Audio Support:
+1.800.374.2440 or
+1.706.645.6500

Pepper Hamilton LLP
Attorneys at Law

Click this icon to view the slide in full screen mode.

BYOD (Bring Your Own Device)...
*Liability and Data Breach Sold Separately

Hit the 'Escape' key to return to the normal view.

December 12, 2013 | Sharon R. Klein, Tracey E. Diamond , Odia Kagan

Pepper Hamilton LLP
Attorneys at Law

1

Feel free to submit text questions throughout the webinar

BYOD (Bring Your Own Device)... *Liability and Data Breach Sold Separately

December 12, 2013 | Sharon R. Klein, Tracey E. Diamond , Odia Kagan

Pepper Hamilton LLP
Attorneys at Law

1

Click this icon to download the slides as a handout

BYOD (Bring Your Own Device)...
*Liability and Data Breach Sold Separately

December 12, 2013 | Sharon R. Klein, Tracey E. Diamond , Odia Kagan

Pepper Hamilton LLP
Attorneys at Law

Speaker: Sharon R. Klein

949.567.3506
kleins@pepperlaw.com

- Partner in the Corporate and Securities Practice Group
- Partner in charge of the firm's Orange County office and chair of the Privacy, Security and Data Protection practice
- Handles a variety of corporate and intellectual property matters, in particular, helping information technology and telemedicine clients grow and succeed
- Commissioner of the Electronic Healthcare Network Accreditation Commission (EHNAC), a voluntary, self-governing standards development organization established to develop standard criteria and accredit organizations that electronically exchange health care data.

Pepper Hamilton LLP
Attorneys at Law

Speaker: Tracey E. Diamond

215.981.4869
diamondt@pepperlaw.com

- Attorney with Pepper Hamilton LLP, resident in the Philadelphia office
- Practices in the areas of employment law, human resources counseling and employment litigation
- Regularly counsels clients on workplace issues, provides harassment training, conducts internal investigations, drafts policies and procedures, negotiates employment and severance agreements, advises on independent contractor, FMLA and ADA compliance issues, and partners with clients to structure their workforce in the most efficient and effective way possible.

Pepper Hamilton LLP
Attorneys at Law

Speaker: Odia Kagan

215.981.4647
kagano@pepperlaw.com

- Associate in the Corporate and Securities Practice Group of Pepper Hamilton LLP, resident in the Philadelphia office
- Experience includes the representation of Israeli and foreign companies in stock and asset acquisitions, mergers, joint ventures, BOT projects and various commercial transactions, as well as Internet and IT law, including the representation of technology and start-up companies from formation in various aspects of doing business in cyberspace
- Prior to joining Pepper, she was a partner in the Tel Aviv, Israel firm Shavit Bar-On Gal-On Tzin Nov Yagur Law Offices and a managing partner of a boutique law firm.

Pepper Hamilton LLP
Attorneys at Law

- BYOD - What?
- BYOD – Why?
- BYOD – Why Not?
- BYOD – How?

BYOD: What?

BYOD: What?

BYOD: What?

- “Bring Your Own Device” - The policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged company information and applications.

BYOD: Where?

- 80% of employees presently use personal technology for business purposes.
- 75% of employees in emerging markets use personal devices at work; 44% in developed markets.
- It is projected that 50% of US employers will stop providing devices to employees by 2017.

BYOD: Where?

…But

- On average only 20.1% of employees who use personal devices have also signed a policy governing that behavior. USA and India are nearer to 50%

BYOD: Why?

- Less expensive.
- Gives the employee the freedom to choose.
- Increases productivity and responsiveness.
- Increases innovation.

BYOD: Why Not?

- 63% of employees use mobile devices to access workplace data, including sensitive regulated data.
- Despite the risk, 67% of organizations have no special policy in place to monitor employees with access to regulated data.
- Only 52% of mobile devices with access to regulated data have adequate security.

BYOD: Why Not?

- Increased Risks with respect to Regulated Data
- Data on BYOD Devices is Discoverable
- Employment Issues

Why Not: Increased Risk for Regulated Data

Are any of the following statements true for your company?

- I don't know how much regulated data is on mobile devices used by my employees or transferred to cloud-based file sharing applications.
- My employees can access regulated data using unsecured mobile devices.
- I am not worried about the risk of having regulated data on mobile devices and it is not a top security priority for me.
- I don't monitor employees who access and use regulated data on mobile devices
- I don't regularly and clearly convey to my employees the importance of protecting regulated data on mobile devices.
- I don't have structured and legally vetted oversight or governance practices in place regarding mobile devices.

Why Not: Increased Risk for Regulated Data

- 54% of organizations have had 5 or more data breach incidents involving a mobile device containing regulated data.
- On average, 6,000 records were lost or stolen in each such data breach.

Why Not?: Discovery - Anything can and will be used against you…

- For the employer:
  - Data is subject to preservation, collection and production requirements.
  - Ready access to the data is more difficult on a private device.
  - Discovery is expensive.
- For the employee:
  - Data on the phone could be examined by the counterparty to the litigation.

eDiscovery To Do's:

- Create logical partitions between work and personal content.
- Develop separate user accounts with separate logins.
- Back up all work-related data on the personal device to an employer-controlled space.

Why Not: SCA Issues

- The SCA may bar an employer from intentionally accessing electronic communications.
- Clear authorization can be a defense.
- Reduce risk by:
  - Having a clear policy in place.
  - Limit employees entitled to BYOD.
  - Train employers on what they can access.
  - Educate employees on scope of authorization.

Why not?
Employment Issues

- Inappropriate behavior through mobile device
- Discrimination
- GINA and ADA
- Overtime
- FMLA
- OSHA and Workers' Comp
- NLRA Issues
- Expense Reimbursement

Employment Issues: Overtime

- More than *de minimis*?
- Tracking
- Enforcement
- Time spent supporting/repairing devices

Employment Issues: OSHA & WC

- “Blackberry Thumb”
- “Text Neck”
- Brain injury from cell signals
- Distracted driving

Employment Issues: NLRA Issues

- Is policy a mandatory subject of bargaining?
- May employer monitor the device?
- Is the employer restraining the employees' ability to engage in concerted activity?

Employment Issues: Expense Reimbursement

- State law requirements for reimbursement of business expenses
- How to determine percentage of cost related to business use vs. personal use

BYOD: How?

- General Steps
- BYOD Policy
  - Training
  - Enforcement
- Other Documents and Policies

BYOD : How? - General Steps

- The security policy should cover regulated data on mobile devices and prohibit circumventing or disabling security features.
- Regulated data on mobile devices should be protected as sensitive and confidential information.
- Conduct a data inventory of confidential information.
- Understand who is accessing confidential data and for what purposes.
- Consider investing in mobile device management, mobile DRM and mobile application management.
- Educate employees on “less is more” strategies.

BYOD Policy Components

- No expectation of privacy
- Employee consent to monitoring
- Employee consent to remote wiping
- Instruction to employee to preserve data
- Prohibit sharing of device
- Must report if lost or stolen
- Prohibit use of cloud-based storage of company data

BYOD Policy Components (cont'd)

- No texting while driving
- Compliance with all other company policies (i.e., harassment, discrimination, overtime, confidentiality)
- Consequences

Other Policies Implicated by BYOD

- Electronic Communications
- Confidentiality
- Code of Conduct
- Return of Company Property
- Intellectual Property
- EEO & Harassment
- Recording Time and Overtime
- Leaves of Absence
- Workplace Safety

Other Employment Documents/Practices Implicated by BYOD

- Employment Agreements
- Separation Agreements
- Independent Contractor Agreements
- Records Management
- Litigation Holds
- Management of Passwords and User ID's

Questions & Answers

Contact Brian Dolan at dolanb@pepperlaw.com for CLE Information

Thank You!

Sharon R. Klein
949.567.3506
kleins@pepperlaw.com

Tracey E. Diamond
215.981.4869
diamondt@pepperlaw.com

Odia Kagan
215.981.4647
kagano@pepperlaw.com

Pepper Hamilton LLP
Attorneys at Law

Pepper Hamilton LLP
Attorneys at Law