VENABLE® LLP

Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know

Wednesday, February 19, 2014, 12:30 p.m. – 2:00 p.m. ET

Venable LLP, Washington, DC

Moderator:
Jeffrey S. Tenenbaum, Esq., Venable LLP

Panelists:
David R. Warner, Esq., Venable LLP
Armand J. (A.J.) Zottola, Esq., Venable LLP

Upcoming Venable Nonprofit Legal Events

March 20, 2014 - The OMB Super Circular: What the New Rules Mean for Nonprofit Recipients of Federal Awards

April 29, 2014 - Election-Year Advocacy: Maintaining Your Nonprofit's Clear Message in Cloudy Legal Seas

VENABLE® LLP

Agenda

- Current Issues
- Overview of BYOD Policies
- Integrating BYOD in Your Workforce
- Lessons from the Front Lines
- Putting It All Together
- Hypothetical Situations
- Takeaways, Tips, and Questions

VENABLE® LLP

Current Issues

VENABLE LLP

What Is "Bring Your Own Device"?

- Central management of the security of personally-owned mobile devices, including smart phones and tablets, to support the following security objectives:
  - Confidentiality: Ensure that transmitted and stored data cannot be read by unauthorized parties
  - Integrity: Detect any intentional or unintentional changes to transmitted and stored data
  - Availability: Ensure that users can access resources using mobile devices whenever needed

See, e.g., NIST Guidelines for Managing the Security of Mobile Devices (800-124).

What Issues Are Presented by BYOD?

- **Hypothetical 1:** During a board meeting, the CEO makes reference to a sensitive document, which he has e-mailed to his personal smartphone from his corporate account.
- **Hypothetical 2:** An employee loses a dual-use device.
- **Hypothetical 3:** An employee's dual-use device is infected with malware.
- **Hypothetical 4:** Your nonprofit is sued and asked to disclose information from an employee's device.

Unsecure Information

- BYOD programs and dual-use devices necessarily involve taking information outside of the protection of an organization's private servers
- Trade secrets must be subject to reasonable efforts to maintain their secrecy
- Devices that are lost, stolen, or used on unsecured networks can result in the loss of information

Did you know: *Between 2009 and 2011, 48 mobile devices were lost or stolen from NASA, including an unencrypted laptop with command and control codes for the International Space Station*

http://oig.nasa.gov/Special-Review/SpecialReview(12-17-12).pdf

Overlap of Work Space and Personal Space

- Employees may store personal information on a dual-use device, complicating security procedures such as remote-wipes and GPS tracking
- Retrieving data and devices from employees that quit or are fired can be complicated
- BYOD policies that do not obtain informed written consent may not be enforceable

Did you know: *In 2010, a publishing company accidentally remote-wiped an employee's dual-use device, destroying her contacts, photos and media, and the phone's ability to make calls.*

http://www.npr.org/2010/11/22/131511381/wipeout-when-your-company-kills-your-iphone

BYOD and Privacy

- Businesses that store consumer information (Social Security, driver's license, credit card, and account numbers) have security obligations, and BYOD expands the area an organization must protect
- A breach of security on an employee's personal device can lead to government enforcement actions, civil penalties, and litigation

Did you know: *The Massachusetts Attorney General has obtained penalties from companies that failed to meet Massachusetts cybersecurity and encryption requirements.*

http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html

VENABLE® LLP

Overview of BYOD Policies

VENABLE® LLP

Outline of a BYOD Policy

- **Parameters:** Define who can participate or are subject to the policy
- **Scope:** What devices? What conduct?
- **Security:** Set boundaries and create both proactive and reactive security processes. Access rights and requirements? What information is accessible or transmittable? When and how are security incidents to be reported?
- **Monitoring:** Address employees' expectations of privacy
- **User Support:** Describe how and where users can get technical support/respond to security incident
- **Policy Violations:** Control unsecured behavior by setting out clear consequences

BYOD Policy and Compliance

- Cybersecurity regulations and guidelines:
  - **HIPAA:** The HIPAA Security Rule requires that covered entities at least consider whether encryption of personal health information, such as medical history, test and laboratory results, and insurance information, in electronic form is feasible and, if not, to document the basis for that conclusion. 45 C.F.R. pt. 164.312(a)(2), (e)(2).
  - **GLB:** Gramm-Leach-Bliley protects information held by financial institutions, such as account and social security numbers. GLB's safeguarding regulations require covered entities to identify risks to the security of customer information (including a risk assessment of computer information systems), and contractually require service providers to implement and maintain safeguards. 16 C.F.R. pt. 314

VENABLE LLP

BYOD Policy and Compliance

- Record keeping rules:
  - Records of communications by an employee pertaining to the firm's business must be maintained, retrievable, and reviewable. SEC Rules 17 a-3 and 17 a-4; NASD Rule 31101.
- Compliance with state laws and rules:
  - California: Imposes a general statutory duty on businesses to safeguard personal information. Cal. Civ. Code § § 1798.80 *et seq.*
  - Massachusetts: Specifically address portable devices, requiring encryption of personal information stored on them. Mass. Regs. Code tit. 201, § § 17.03 – 17.04.
  - Texas: Imposes a general statutory duty on businesses to safeguard personal information. Tex. Bus. & Com. Code tit. 11, § 521.

VENABLE® LLP

Additional Policy Considerations

- Existing trade secret or email/computer policies
- Existing EEO, collective bargaining, and other policies
- Guidelines for configuring devices
- Particular response to a data breach
- Guidelines and processes for litigation (such as preserving and deleting data)
- Safety (for example, a policy against using a device while operating a vehicle)
- Training

VENABLE® LLP

Integrating BYOD in Your Workforce

Overview

- Management Issues
- Equal Employment and BYOD
- Wage and Hour Issues
- Workplace Safety and Health
- Unionized Workforce
- International Considerations

VENABLE LLP

Management Issues

- BYOD has the potential to expand the scope of employment
- BYOD combines the workplace with the private sphere
  - Information about employees' private lives
  - Use of devices by employee's family and friends
- "Devices" are not simply phones, but combine a broad range of abilities and activities
  - For example, apps for diabetes management

Equal Employment Opportunity and BYOD

- Translating current organization policies to BYOD (for example, harassment policies)
- Developing new policies to cover quasi-work environments
- Accommodating people with disabilities

Wage and Hour Issues

- Off-the-clock work and overtime
- Employee reimbursement (state law reimbursement requirements)
- Tracking usage of dual-use devices

Workplace Safety and Health

- OSHA regulations and BYOD
  - Distracted driving: Work-related texting and e-mailing while driving
  - Repetitive stress injuries

VENABLE® LLP

Unionized Workforce

- BYOD policies may be covered by and subject to collective bargaining agreements

International Considerations

- Border searches:
  - Devices can be searched and detained without a suspicion of criminal activity
  - Consent is not required
- Foreign wage-hour laws: The EU has stricter wage-hour laws than the United States, requiring separate or additional controls
- International privacy laws: Device monitoring and security measures must be evaluated under multiple privacy regimes

VENABLE® LLP

Lessons from the Front Lines

Challenges in Drafting a BYOD Policy

- Multiple stakeholders
- Traditional notions of enterprise IT structure
- Employee perceptions
- Uncertain legal landscape
- Achieving employee compliance

VENABLE® LLP

The Culture of BYOD

- Reflecting organization culture/risk tolerance
- Ownership does NOT equal expectation of privacy
- Building Success: Weaving BYOD into existing policies
- Training

VENABLE® LLP

An Ongoing Effort

- Rapid changes in devices/platforms and capabilities (phones, tablets, “phablets,” etc.)
- Increase in third-party software and access points
- Devices often defined/demanded by employees
- Flexible/coordinated review process

VENABLE LLP

Closing Observations

- Implementation is key: Active management/dedicated resources
- Use technology to control technology
- Data Loss Prevention (DLP) is a primary concern
- Productivity

VENABLE® LLP

Putting It All Together

VENABLE LLP

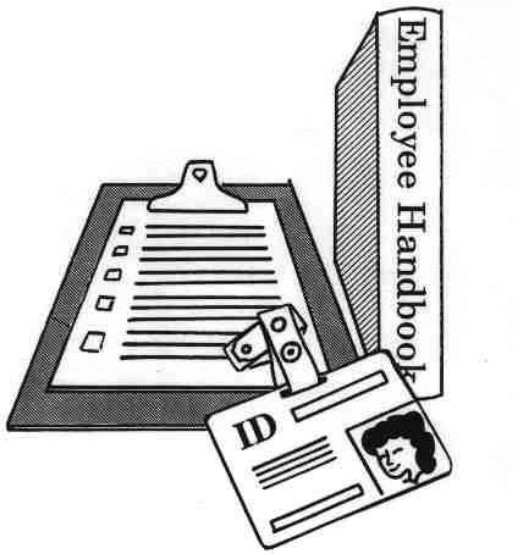
Putting It All Together

- Goals of a BYOD Policy:
  - Setting expectations
    - Draw lines between work use and private use
    - Develop awareness around BYOD issues
  - Meeting compliance requirements
    - HIPAA
    - SEC
    - GLB
  - Avoiding undue cost, risk, and liability
    - Litigation and discovery
    - Equal Employment considerations
    - Protecting trade secrets

VENABLE LLP

Translating Goals and Risks into a BYOD Policy

- Address current and anticipated risks
- Obtain informed employee written consent, and involve employees in the Policy through training
- Keep the Policy adaptable to meet unexpected challenges



VENABLE LLP

Keep an Eye on the Future

- Stay current with BYOD-related laws, regulations, and trends
  - Federal legislation
  - State laws (for example, California)
- Follow the development of cybersecurity and BYOD-specific guidelines
  - NIST Framework
  - NIST Guidelines for Managing the Security of Mobile Devices (Special Publication 800-124)
  - EU Privacy Directives and Proposed GDPR
- Keep your BYOD Policy active
  - Address changes in law and culture
  - Investigate additional solutions (such as cyber-insurance)

VENABLE® LLP

Hypothetical Situations

VENABLE LLP

Hypothetical One:

- Your nonprofit does not have a BYOD policy. During a board meeting, the CEO makes reference to a sensitive corporate document. To make his point, the CEO pulls out his personal smartphone and opens a copy of the document, which he had e-mailed to himself from his corporate account.

Did you know: *The Corporate Executive Board in April 2013 released a survey of 165,000 employees showing "93 percent of workers knowingly violate policies designed to prevent data breaches, and senior executives are the worst offenders."*

See Financial Times, available at: http://www.ft.com/cms/s/0/01f936e6a365-11e2-ac00-00144feabdc0.html#axzz2mgg9Cvc1

Hypothetical Two:

- An employee loses a dual-use device; how does your organization respond and does the BYOD policy address the situation?

Did you know: *In 2012, a stolen laptop with unencrypted data, including 3,621 patients' information, cost Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. $1.5 million in fines.*

See FierceHealthIT, available at: http://www.fiercehealthit.com/story/boston-teaching-hospital-fined-15mephi-data-breach/2012-09-18

Hypothetical Three:

- An employee's dual-use device is infected with malware; how does your organization respond and does the BYOD policy address the situation?

Did you know: *In 2012, a breach at St. Mark's Medical Center in La Grange, TX reported that an employee-owned computer was infected by malware. On it was patient information like names, Social Security numbers, and dates of birth of almost 2900 patients.*

See PHIprivacy.net, available at: http://www.phiprivacy.net/st-marks-medical-center-notifies-patients-after-finding-malware-on-system/

Hypothetical Four:

- Your organization is sued and asked to disclose information from an employee's device; how does your organization respond and does the BYOD policy address the situation?

Did you know: *In E.E.O.C. v. Original Honeybaked Ham Co. of Georgia, the U.S. District Court for the District of Colorado ordered the collection and in camera review of plaintiffs' Facebook, blog post and cell phone data in a class action sexual harassment suit. When the EEOC failed to comply with this eDiscovery Rule, the Federal District Court in Colorado granted a motion for sanctions under FRCP 16(f). The court held the plaintiffs did not engage in bad faith, but did "engage in some kind of unreasonable or obstreperous conduct that delays the discovery process."*

E.E.O.C. v. Original Honeybaked Ham Co. of Georgia, 11-cv-02560 (D. Colo. Nov. 7, 2012) [2012 WL 5430974; 2012 U.S. Dist. LEXIS 160285].

VENABLE® LLP

Takeaways, Tips, and Questions

VENABLE LLP

Ensure a "Triple A" BYOD Policy

- Awareness
  - Stage One: All parts of organization leadership, executive, legal, and IT, must agree on the need for a Policy
  - Stage Two: Users must know about the Policy and the BYOD program in general
- Acceptance
  - Users must accept a BYOD program, through informed written consent
- Action
  - The BYOD policy is only a starting point, it must be actively used, revised, and improved

VENABLE® LLP

Key BYOD Policy Considerations

1. **Policy:** Ensure you have a BYOD policy.
2. **Focus:** Draft for “YOUR” organization.
3. **Clarify Expectations:** Clearly define work use and private use.
4. **Informed Consent:** Employees must expressly accept how and for what purpose the organization may access their devices.
5. **Connections:** Consider how your employees connect remotely.
6. **Information:** Consider what kind of data will be accessible or transmitted.
7. **Compliance:** Consider statutory, regulatory, and contractual requirements.
8. **Training:** Keep BYOD users up-to-date on acceptable uses for dual-use devices.
9. **Monitoring:** Consider how dual-use devices will be monitored.
10. **Stay Current:** Be aware of new technology and regulations.

VENABLE LLP

Questions?

Jeffrey S. Tenenbaum, Esq.
jstenenbaum@Venable.com
t 202.344.8138

David R. Warner, Esq.
drwarner@Venable.com
t 703.760.1652

Armand J. (A.J.) Zottola, Esq.
ajzottola@Venable.com
t 202.344.8546

To view Venable's index of articles, presentations, recordings and upcoming seminars on nonprofit legal topics, see www.Venable.com/nonprofits/publications, www.Venable.com/nonprofits/recordings, www.Venable.com/nonprofits/events.