

BYOD for 501(c)s: Pros and Perils of “Bring Your Own Device”

April 3, 2014, 2:00 p.m. ET

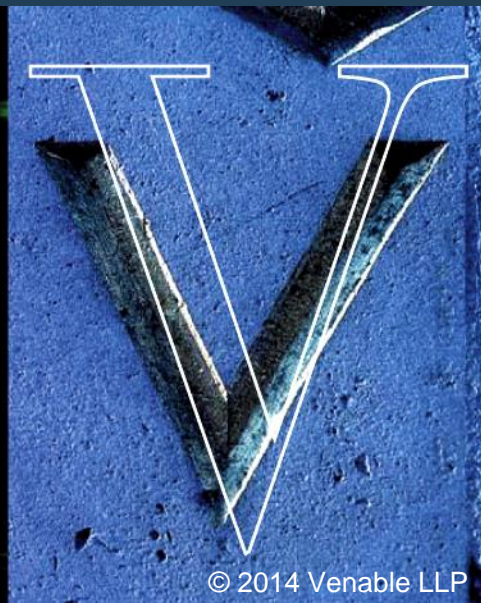
Moderator:

Jeffrey S. Tenenbaum, Esq., Venable LLP

Panelists:

Ronald W. Taylor, Esq., Venable LLP

Armand J. (A.J.) Zottola, Esq., Venable LLP



Panelist Biographies

Ronald W. Taylor, Venable LLP



Ron Taylor heads Venable's Maryland Labor and Employment Practice Group and its national OSHA practice. Mr. Taylor has been repeatedly listed in Chambers USA: America's Leading Lawyers for Business, Best Lawyers in America, and Maryland Super Lawyers as one of the leading employment lawyers in Maryland. He was recently selected as one of the top 100 lawyers in Maryland and has been described as one of the most recognized lawyers in the field, noted for his sound judgment and ability to resolve problems efficiently with good results for his clients as well as for his experience with occupational safety and health law. He is a fellow of the prestigious College of Labor and Employment Lawyers.



Panelist Biographies

Armand J. (A.J.) Zottola, Venable LLP



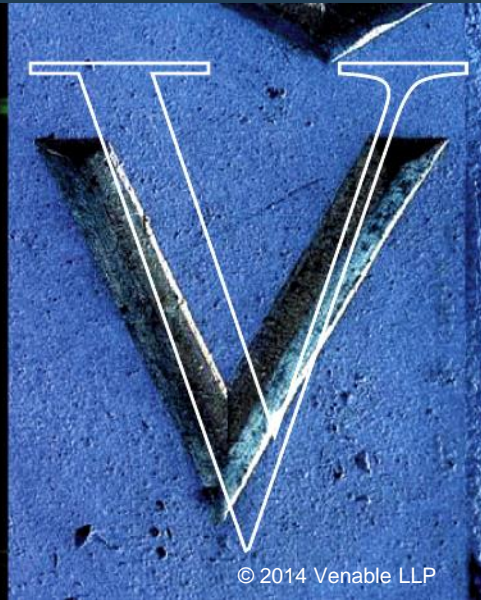
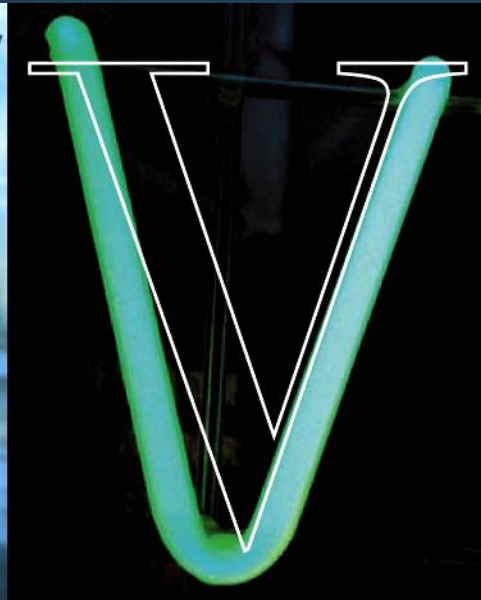
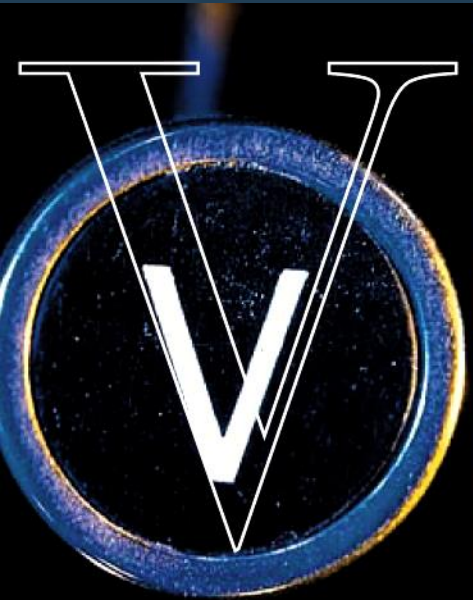
Working at the intersection of commerce and technology, A.J. Zottola focuses his practice on the exploitation of intellectual property, intangible and technology assets in business and strategic relationships. His extensive experience also helps clients resolve and craft settlement arrangements for misappropriation and infringement matters and for disputes involving commercial and licensing agreements. In addition, he regularly counsels clients on

intellectual property, e-commerce and privacy issues, and prosecutes and manages U.S. and foreign trademark and copyright portfolios.

His in-depth technology knowledge, recognized by BEST LAWYERS, LEGAL 500, and CHAMBERS, helps clients achieve practical and creative solutions to procure, exploit, manage and protect their intangible and proprietary assets. Whether resolving employer/employee intellectual property ownership issues, assessing new technology developments, or acquiring technology assets through mergers and acquisitions, Mr. Zottola assists a variety of companies and funding sources in maximizing asset value, identifying new opportunities for business expansion and generation, and preventing the unwanted loss or infringement of proprietary rights.



Current Issues



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 emailed 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 is 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 a company's private servers
- Trade secrets must be subject to reasonable efforts to maintain its 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](http://oig.nasa.gov/Special-Review/SpecialReview(12-17-12).pdf)



Overlap of Workspace 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

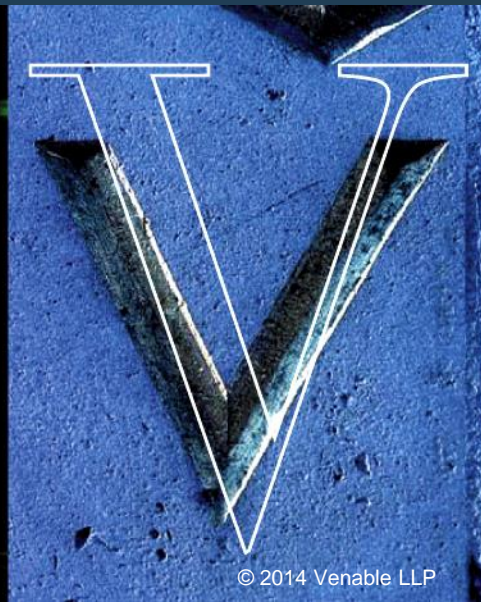
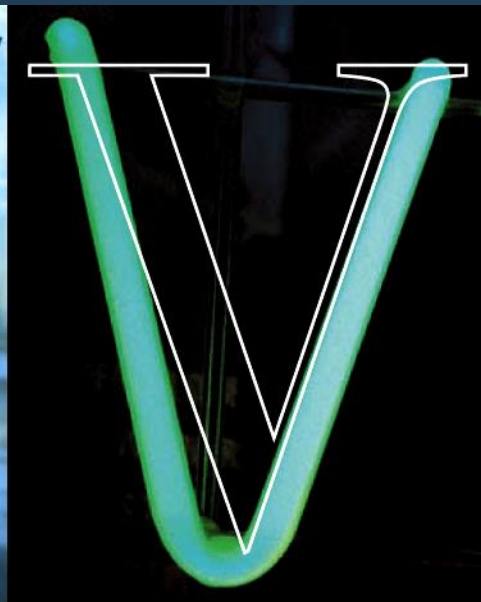
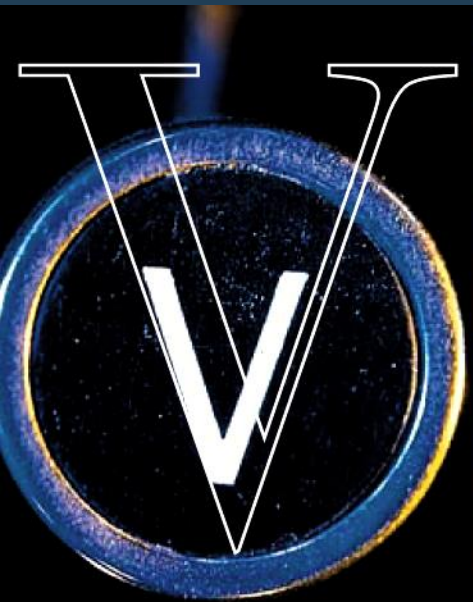
- Businesses that store consumer information (Social Security, driver's license, credit card, and account numbers) have security obligations, and BYOD expands the area a company must protect
- A breach of security on an employee's personal device can lead to government enforcement actions, civil penalties,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



Overview of BYOD Policies



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. GLBA's safeguarding regulations requires 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



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 addresses 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. and Com. Code tit. 11, § 521

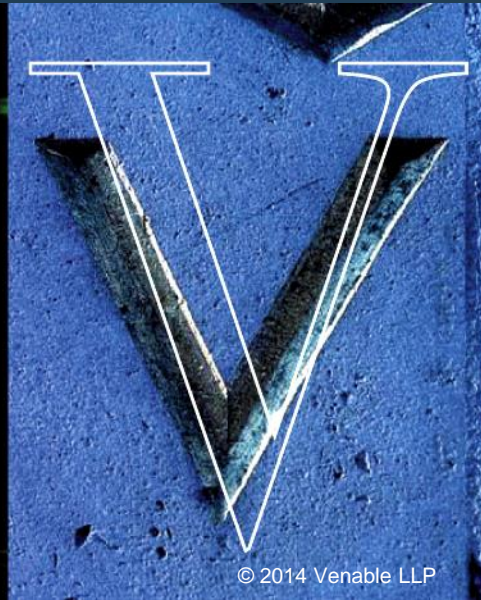
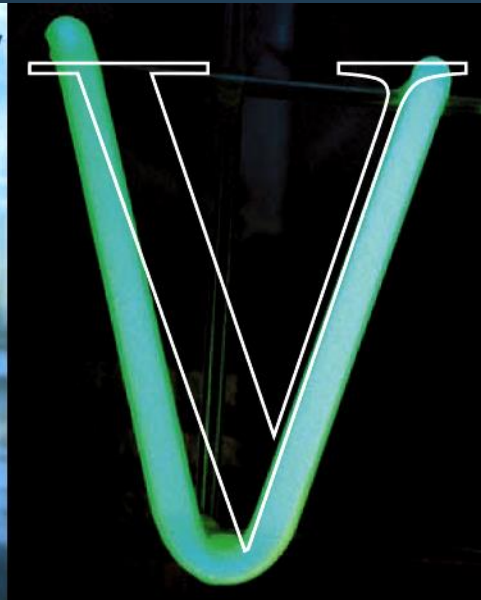
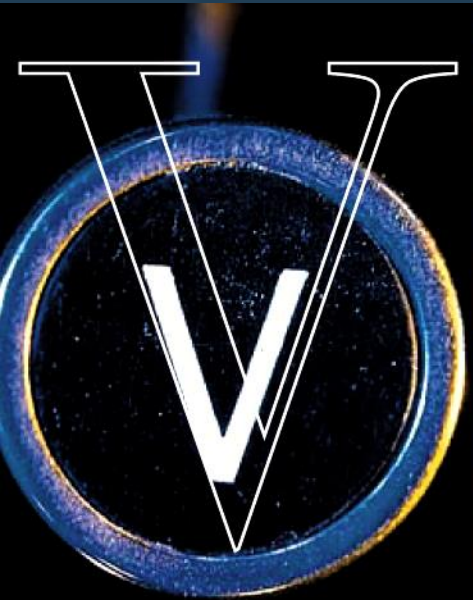


Additional Policy Considerations

- 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



Integrating BYOD in Your Workforce



Overview

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



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 employees' families 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

- Translating current company 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 emailing while driving
 - Repetitive stress injuries



Unionized Workforce

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

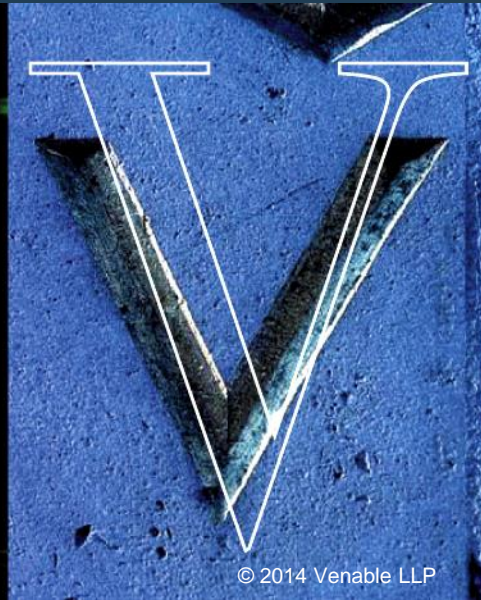
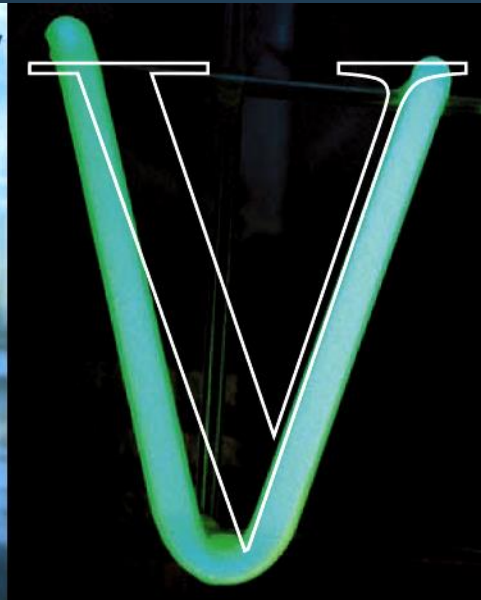
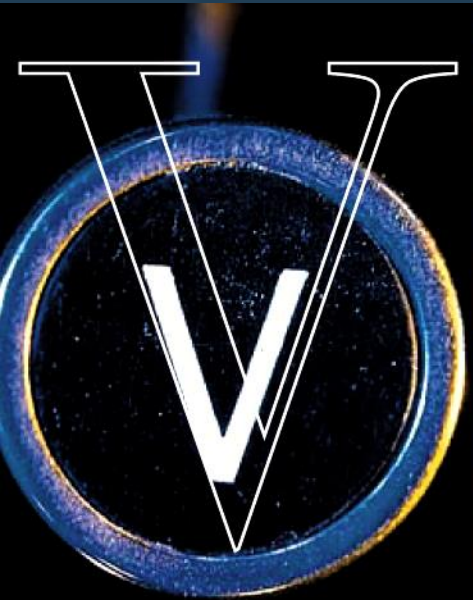


International Considerations

- 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



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



The Culture of BYOD

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



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



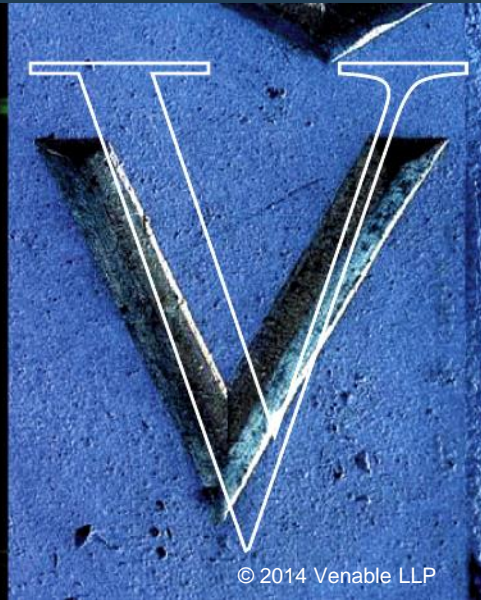
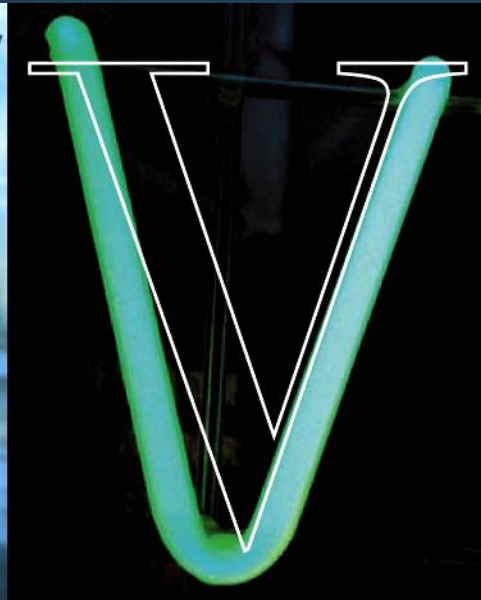
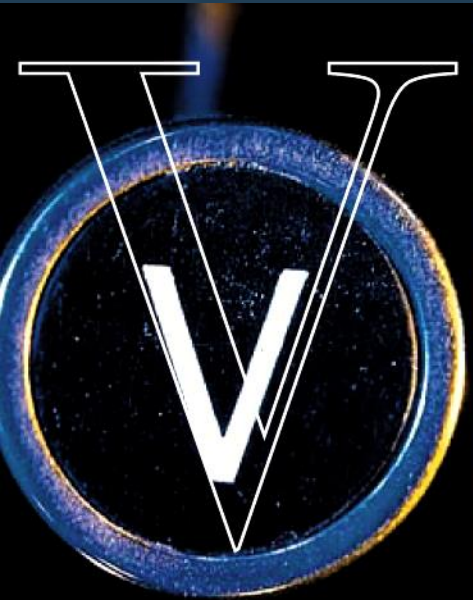
Closing Observations

- 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



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



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

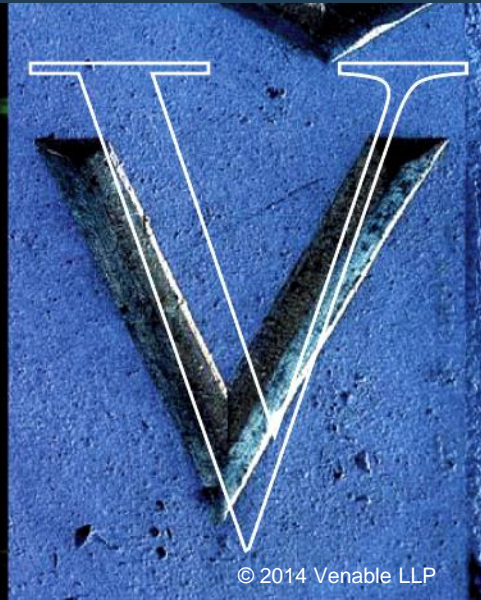
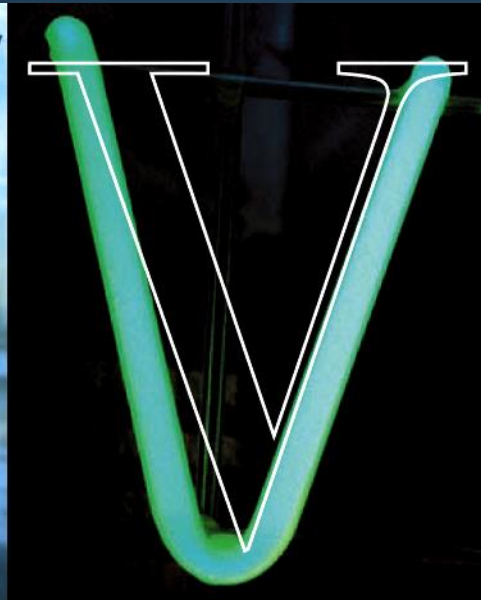
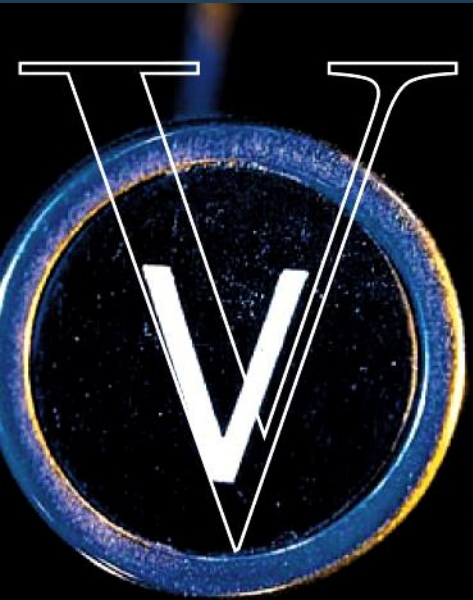


Keep an Eye on the Future

- 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)



Takeaways and Questions



Ensure a “Triple A” BYOD Policy

- Awareness
 - Stage One: All parts of company 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



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.



Questions?

Jeffrey S. Tenenbaum, Esq.

jstenenbaum@Venable.com

t 202.344.8138

Ronald W. Taylor, Esq.

rwaylor@Venable.com

t 410.244.7654

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.

