VENABLE® LLP

ACC AMERICA
Association of Corporate Counsel
WMACCA Chapter

WMACCA Technology and IP Forum

Making Nice with Bring Your Own Device - Tips for Successfully Implementing a BYOD Policy

December 12, 2013

VENABLE® LLP

WMACCA Technology and IP Forum

Making Nice with Bring Your Own Device - Tips for Successfully Implementing a BYOD Policy

Moderator:

Keir X. Bancroft
Associate, Government Contracts Practice Group, Venable LLP

Panelists:

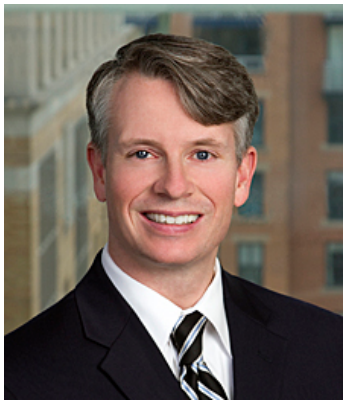
Armand J. (A.J.) Zottola
Partner, Technology Transactions and Outsourcing, Venable LLP

Robert Bethea
Assistant General Counsel, Platforms and Technology, AOL

David Warner
Partner, Labor and Employment, Venable LLP

Biographies

Keir X. Bancroft, Venable LLP - Moderator



Keir Bancroft provides a range of services to clients throughout the government contracting sector, addressing the needs of small, mid-sized and large businesses. Within the broad rubric of cybersecurity, Mr. Bancroft specializes in information security and privacy compliance. He advises clients on compliance with standards promulgated under the Federal Information Security Act ("FISMA"), Federal Information Processing Standards ("FIPS"), the Department of Defense Information Assurance guidelines, the Privacy Act, and similar requirements.

Mr. Bancroft also focuses on national security and industrial security issues arising under the National Industrial Security Program Operating Manual ("NISPOM"), including employee security clearance, reporting obligations, and foreign ownership, control, and influence ("FOCI").

Mr. Bancroft formerly served as an attorney advisor and the privacy officer at the United States Department of the Treasury, Bureau of Engraving and Printing. There, he counseled and represented the Bureau in all facets of federal procurement and was responsible for ensuring Bureau systems complied with privacy and information security requirements.

Panelist Biographies

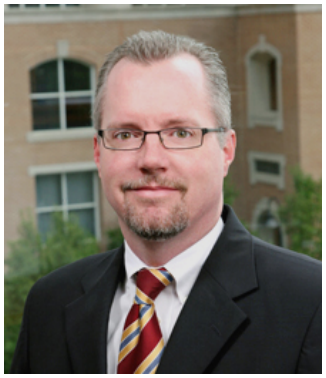
Armand J. (A.J.) Zottola, Venable LLP

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 knowledge 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.

Panelist Biographies

David R. Warner, Venable LLP



David Warner's practice focuses on the resolution and litigation of complex labor, employment, and business disputes. He represents and counsels both private and public sector clients, with a particular emphasis on the government contractor and nonprofit industries.

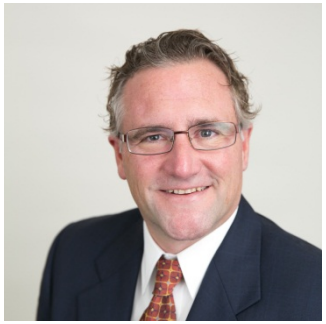
Business Litigation: Mr. Warner routinely represents companies in commercial litigation matters, often concerning the enforcement of management rights in regard to restrictive covenants, trade secrets, business conspiracy and procurement integrity laws.

Employment Counseling: Mr. Warner's practice includes counseling employers on labor and employment related matters in order to minimize potential litigation risk. In addition to day-to-day counseling on employment actions, Mr. Warner provides guidance regarding the design and implementation of effective and defensible application, hiring, promotion, and compensation practices, including conducting comprehensive audits of personnel practices to proactively identify and remediate issues that could give rise to class claims

Employment Litigation: Mr. Warner routinely represents employers in litigation concerning alleged violations of the FLSA and state wage and hour laws, Title VII, the ADA, ADEA, and other federal and state laws prohibiting discrimination and retaliation. Mr. Warner's litigation experience includes complex class action litigation, brought by both private claimants and government agencies, involving extensive electronic discovery and statistical analyses.

Panelist Biographies

Robert Bethea, AOL



Robert Bethea is an Assistant General Counsel at AOL Inc. where he serves as the legal advisor for AOL's Chief Technology Officer and Technology Organization. Having been at AOL for over eight years, Mr. Bethea has consulted on a wide variety of issues and agreements relating to the Internet and AOL's operations and products, including privacy, web site terms of service, cloud agreements, regulatory issues, intellectual property, security, open source, mobile applications, hosting, colocation, and network service agreements, hardware acquisitions, data center, and technology and software licensing (both inbound and outbound). He also provides counsel to the Chief Information Officer and the CIO organization, which is responsible for technology implementations for AOL's Legal Department, and has advised on issues relating to employee conduct and technology policies, including Bring Your Own Device policies. Prior to joining AOL, Mr. Bethea was in private practice where he focused on international trade controls and commercial litigation. He holds a J.D. from the University of Oklahoma and a Master of Laws degree in International and Comparative Law from Georgetown University Law Center

VENABLE® LLP

Introductions and Agenda

- Current Issues
- Overview of BYOD Policies
- Integrating BYOD in Your Workforce
- Lessons From the Front Lines
- Hypothetical Situations
- Takeaways, Tips, and Questions

VENABLE® LLP

Current Issues

Keir Bancroft

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).

VENABLE LLP

What Issues Are Presented by BYOD?

- **Hypothetical 1:** During a board meeting, the CEO makes reference to a sensitive corporate 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 company is sued and is asked to disclose information from an employee's device.

VENABLE® LLP

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

VENABLE LLP

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 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

VENABLE® LLP

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

VENABLE® LLP

Overview of BYOD Policies

A.J. Zottola

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/transmittable?
- **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

VENABLE LLP

BYOD Policy and Compliance

- **Cybersecurity regulations and guidelines:**
  - HIPPA: The HIPPA 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

VENABLE LLP

BYOD Policy and Compliance

- **Government Contracting and FISMA rules:**

  Government contractors may be held to a higher/stricter standard when dealing with government data

  - NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices.
  - OMB M-12-20 (All federal requirements for data protection and remote access are applicable to mobile devices).
  - OMB Circular A-130 (NIST standards apply)
  - OMB M-06-16 (encryption)
- **Cybersecurity Framework for Critical Infrastructure:**
  - Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*
  - NIST Cybersecurity Framework

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
- 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

David Warner

VENABLE® LLP

Overview

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

Management Issues

- BYOD has the potential to expand the scope of employment
- BYOD combines the workplace with the private sphere
- “Devices” are not simply phones, but combine a broad range of abilities and activities

VENABLE® LLP

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 & Hour Issues

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

VENABLE® LLP

Workplace Safety & Health

- OSHA regulations and BYOD
  - Distracted Driving: Work-related texting and e-mailing while driving
  - Repetitive Stress Injuries

VENABLE LLP

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

Robert Bethea

VENABLE LLP

Challenges in Drafting a BYOD Policy

- Multiple Stakeholders
- Traditional Notions of Enterprise IT Structure
- Employee Perceptions
- Uncertain Legal Landscape

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)
- 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
    - FISMA
    - HIPPA
    - SEC
    - GLB
    - NIST Framework
  - 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 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 company 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 per cent 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

VENABLE® LLP

Hypothetical Two:

- An employee loses a dual-use device, how does your company 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

VENABLE® LLP

Hypothetical Three:

- An employee's dual-use device is infected with malware, how does your company 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 date of births 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 company is sued and is asked to disclose information from an employee's device, how does your company 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 and Questions

VENABLE LLP

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 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 and Comments

Keir Bancroft
Venable LLP
kxbancroft@Venable.com
t 202.344.4826
f 202.344.8300

A.J. Zottola
Venable LLP
ajzottola@Venable.com
t 202.344.8546
f 202.344.8300

David Warner
Venable LLP
drwarner@Venable.com
t 703.760.1652
f 703.821.8949

www.Venable.com

VENABLE® LLP

References and Resources

- HIPPA Security Rule, 45 C.F.R. pt. 164.312(a)(2), (e)(2). Available at: http://www.gpo.gov/fdsys/pkg/CFR-2012-title45-vol1/xml/CFR-2012-title45-vol1-sec164-312.xml
- Gramm-Leach-Bliley Safeguarding Regulations, 16 C.F.R. pt. 314. Available at: http://www.gpo.gov/fdsys/pkg/CFR-2009-title16-vol1/pdf/CFR-2009-title16-vol1-part314.pdf
- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*: Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- NIST Cybersecurity Framework: Guidelines for Managing the Security of Mobile Devices. Available at: http://www.nist.gov/itl/cyberframework.cfm

VENABLE LLP

References and Resources

- OMB Circular A-130. Available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4
- OMB M-13-20. Available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-20.pdf
- OMB M-06-16. Available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
- SEC Rules 17 a-3, 17 a-4. Available at: http://www.gpo.gov/fdsys/pkg/CFR-2012-title17-vol3/pdf/CFR-2012-title17-vol3-part240.pdf
- NASD Rule 3110. Available at: http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3734

VENABLE® LLP

References and Resources

- California Cal. Civ. Code § § 1798.80 et seq., statutory duty to safeguard personal information. Available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
- Massachusetts Regs. Code tit. 201, § § 17.03 – 17.04, requiring encryption of personal information on portable devices. Available at: http://www.lawlib.state.ma.us/source/mass/cmr/201cmr.html
- Texas Tex. Bus. & Com. Code tit. 11, § 521, statutory duty to safeguard personal information. Available at: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm