VENABLE® LLP

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

February 19, 2014

Venable LLP

Washington, DC

Moderator:

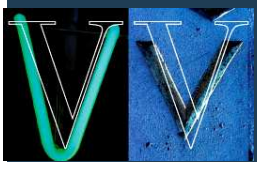
Jeffrey S. Tenenbaum, Esq., Venable LLP

Panelists:

David R. Warner, Esq., Venable LLP

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

Presentation



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

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

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

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 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.

VENABLE LLP

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

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 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

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 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

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

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.

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

VENABLE LLP

Overview

- Management Issues
- Equal Employment and BYOD
- Wage and Hour Issues
- 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 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

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

VENABLE® LLP

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

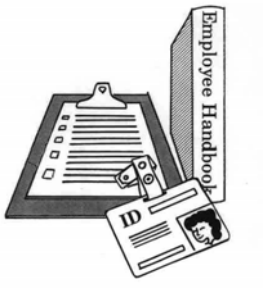
Putting It All Together

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)

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

VENABLE LLP

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

VENABLE LLP

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/

VENABLE LLP

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

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?

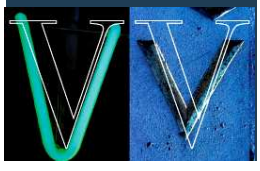
Jeffrey S. Tenenbaum, Esq.
jstenenbaum@Venable.com
t 202.344.8138

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.

Speaker Biographies



VENABLE® LLP

our people

Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

jstenenbaum@Venable.com

Jeffrey Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. He is one of the nation's leading nonprofit attorneys, and also is an accomplished author, lecturer, and commentator on nonprofit legal matters. Based in the firm's Washington, DC office, Mr. Tenenbaum counsels his clients on the broad array of legal issues affecting charities, foundations, trade and professional associations, think tanks, advocacy groups, and other nonprofit organizations, and regularly represents clients before Congress, federal and state regulatory agencies, and in connection with governmental investigations, enforcement actions, litigation, and in dealing with the media. He also has served as an expert witness in several court cases on nonprofit legal issues.

Mr. Tenenbaum was the 2006 recipient of the American Bar Association's Outstanding Nonprofit Lawyer of the Year Award, and was an inaugural (2004) recipient of the *Washington Business Journal*'s Top Washington Lawyers Award. He was one of only seven "Leading Lawyers" in the Not-for-Profit category in the prestigious 2012 *Legal 500* rankings, and one of only eight in the 2013 rankings. Mr. Tenenbaum was recognized in 2013 as a Top Rated Lawyer in Tax Law by *The American Lawyer* and *Corporate Counsel*. He was the 2004 recipient of The Center for Association Leadership's Chairman's Award, and the 1997 recipient of the Greater Washington Society of Association Executives' Chairman's Award. Mr. Tenenbaum was listed in the 2012-14 editions of *The Best Lawyers in America* for Non-Profit/Charities Law, and was named as one of Washington, DC's "Legal Elite" in 2011 by *SmartCEO Magazine*. He was a 2008-09 Fellow of the Bar Association of the District of Columbia and is AV Peer-Review Rated by *Martindale-Hubbell*. Mr. Tenenbaum started his career in the nonprofit community by serving as Legal Section manager at the American Society of Association Executives, following several years working on Capitol Hill as a legislative assistant.

AREAS OF PRACTICE

Tax and Wealth Planning
Antitrust
Political Law
Business Transactions Tax
Tax Controversies and Litigation
Tax Policy
Tax-Exempt Organizations
Wealth Planning
Regulatory

INDUSTRIES

Nonprofit Organizations and Associations
Credit Counseling and Debt Services
Financial Services
Consumer Financial Protection Bureau Task Force

GOVERNMENT EXPERIENCE

Legislative Assistant, United States House of Representatives

BAR ADMISSIONS

District of Columbia

REPRESENTATIVE CLIENTS

AARP
Air Conditioning Contractors of America
American Academy of Physician Assistants
American Alliance of Museums
American Association for the Advancement of Science
American Bar Association
American Bureau of Shipping
American Cancer Society
American College of Radiology
American Institute of Architects
American Society for Microbiology
American Society for Training and Development
American Society of Anesthesiologists
American Society of Association Executives

EDUCATION

J.D., Catholic University of America, Columbus School of Law, 1996

B.A., Political Science, University of Pennsylvania, 1990

MEMBERSHIPS

American Society of Association Executives

California Society of Association Executives

New York Society of Association Executives

Association for Healthcare Philanthropy
Association of Corporate Counsel
Association of Private Sector Colleges and Universities
Automotive Aftermarket Industry Association
Biotechnology Industry Organization
Brookings Institution
Carbon War Room
The College Board
CompTIA
Council on CyberSecurity
Council on Foundations
CropLife America
Cruise Lines International Association
Design-Build Institute of America
Foundation for the Malcolm Baldrige National Quality Award
Gerontological Society of America
Goodwill Industries International
Graduate Management Admission Council
Homeownership Preservation Foundation
Human Rights Campaign
Independent Insurance Agents and Brokers of America
Institute of International Education
International Association of Fire Chiefs
International Sleep Products Association
Jazz at Lincoln Center
LeadingAge
Lincoln Center for the Performing Arts
Lions Club International
Money Management International
National Association for the Education of Young Children
National Association of Chain Drug Stores
National Association of College and University Attorneys
National Association of Music Merchants
National Athletic Trainers' Association
National Board of Medical Examiners
National Coalition for Cancer Survivorship
National Defense Industrial Association
National Fallen Firefighters Foundation
National Fish and Wildlife Foundation
National Hot Rod Association
National Propane Gas Association
National Quality Forum
National Retail Federation
National Student Clearinghouse
The Nature Conservancy
NeighborWorks America
Peterson Institute for International Economics
Professional Liability Underwriting Society
Project Management Institute
Public Health Accreditation Board
Public Relations Society of America
Recording Industry Association of America
Romance Writers of America
Trust for Architectural Easements
The Tyra Banks TZONE Foundation
United Nations High Commissioner for Refugees
Volunteers of America

HONORS

Recognized as "Leading Lawyer" in the 2012 and 2013 editions of *Legal 500*, Not-For-Profit

Listed in *The Best Lawyers in America* for Non-Profit/Charities Law, Washington, DC (Woodward/White, Inc.), 2012-14

Recognized as a Top Rated Lawyer in Taxation Law in *The American Lawyer* and *Corporate Counsel*, 2013

Washington DC's Legal Elite, *SmartCEO Magazine*, 2011

Fellow, Bar Association of the District of Columbia, 2008-09

Recipient, American Bar Association Outstanding Nonprofit Lawyer of the Year Award, 2006

Recipient, *Washington Business Journal* Top Washington Lawyers Award, 2004

Recipient, The Center for Association Leadership Chairman's Award, 2004

Recipient, Greater Washington Society of Association Executives Chairman's Award, 1997

Legal Section Manager / Government Affairs Issues Analyst, American Society of Association Executives, 1993-95

AV® Peer-Review Rated by *Martindale-Hubbell*

Listed in *Who's Who in American Law* and *Who's Who in America*, 2005-present editions

ACTIVITIES

Mr. Tenenbaum is an active participant in the nonprofit community who currently serves on the Editorial Advisory Board of the American Society of Association Executives' *Association Law & Policy* legal journal, the Advisory Panel of Wiley/Jossey-Bass' *Nonprofit Business Advisor* newsletter, and the ASAE Public Policy Committee. He previously served as Chairman of the *AL&P* Editorial Advisory Board and has served on the ASAE Legal Section Council, the ASAE Association Management Company Accreditation Commission, the GWSAE Foundation Board of Trustees, the GWSAE Government and Public Affairs Advisory Council, the Federal City Club Foundation Board of Directors, and the Editorial Advisory Board of Aspen's *Nonprofit Tax & Financial Strategies* newsletter.

PUBLICATIONS

Mr. Tenenbaum is the author of the book, *Association Tax Compliance Guide*, now in its second edition, published by the American Society of Association Executives. He also is a contributor to numerous ASAE books, including *Professional Practices in Association Management*, *Association Law Compendium*, *The Power of Partnership*, *Essentials of the Profession Learning System*, *Generating and Managing Nondues Revenue in Associations*, and several Information Background Kits. In addition, he is a contributor to *Exposed: A Legal Field Guide for Nonprofit Executives*, published by the Nonprofit Risk Management Center. Mr. Tenenbaum is a frequent author on nonprofit legal topics, having written or co-written more than 500 articles.

SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer on nonprofit legal topics, having delivered over 500 speaking presentations. He served on the faculty of the ASAE Virtual Law School, and is a regular commentator on nonprofit legal issues for *NBC News*, *The New York Times*, *The Wall Street Journal*, *The Washington Post*, *Los Angeles Times*, *The Washington Times*, *The Baltimore Sun*, *ESPN.com*, *Washington Business Journal*, *Legal Times*, *Association Trends*, *CEO Update*, *Forbes Magazine, The Chronicle of Philanthropy, The NonProfit Times* and other periodicals. He also has been interviewed on nonprofit legal topics on Fox 5 television's (Washington, DC) morning news program, Voice of America Business Radio, Nonprofit Spark Radio, and The Inner Loop Radio.

VENABLE® LLP

our people

David R. Warner

Partner — *Tysons Corner, VA Office*

T 703.760.1652 F 703.821.8949 drwarner@Venable.com

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. Representative engagements include:

- Lead counsel in $21 million breach of service contract action
- Lead counsel in $8 million breach of teaming agreement action
- Lead counsel for government contractor in breach of contract, Unfair Trade Practices Act, and fraud claims against prime contractor; matter resolved before filing of complaint with full recovery to client
- Lead counsel in prosecution of breach of duty of loyalty and trade secret claims against medical supply sales representative in Maryland
- Representation of telecommunications contractor in prosecution of business conspiracy, copyright, breach of duty of loyalty, and trade secrets claims against former employee and competitor; matter resolved prior to trial with more than $4 million paid to client

Government Contractor Compliance and Audits: Mr. Warner has extensive experience advising government contractors in compliance matters, audits, and litigation with the federal government regarding E.O. 11246, the Davis-Bacon Act and Service Contract Act. Representative engagements include:

- Lead attorney in negotiation of 75% reduction of multi-million dollar back pay demand (levied prior to client's engagement of Venable) on behalf of one of the fifty largest private employers in the United States; directed compliance efforts resulting in successful conclusion of multi-year conciliation agreement
- Lead attorney in successful resolution of defense contractor audit, which included significant issues concerning pay equity in salaried ranks
- Lead attorney in training of executives and senior leadership regarding affirmative action, diversity, and talent management best practices at Fortune 100 company
- Represented multi-billion dollar services company in successful resolution of OFCCP glass ceiling audit
- Represented national financial services company in defense of claims of systemic hiring discrimination brought by OFCCP
- Represented multi-billion dollar food manufacturing company in successful resolution of OFCCP glass ceiling audit

Employment Counseling: Mr. Warner's practice includes counseling employers on

AREAS OF PRACTICE

Labor and Employment

Financial Services Wage Compliance

Regulatory

Insurance

Insurance Coverage and Disputes

INDUSTRIES

Government Contractors

Nonprofit Organizations and Associations

BAR ADMISSIONS

Virginia

District of Columbia

Maryland

COURT ADMISSIONS

U.S. District Court for the District of Maryland

U.S. District Court for the District of Columbia

U.S. Court of Appeals for the Fourth Circuit

U.S. District Court for the Northern District of Florida

EDUCATION

J.D., *cum laude*, Georgetown University Law Center, 1996

Editor, Articles and Notes, *American Criminal Law Review*

B.A., *cum laude*, Georgetown University, 1993

MEMBERSHIPS

American Bar Association

Maryland Bar Association

Virginia Bar Association

District of Columbia Bar Association

Maryland Defense Counsel, Inc.

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. Mr. Warner also advises companies in cross-border employment matters, including the design and implementation of expatriate employment agreements, application of U.S. laws to foreign-based employees, and related issues. Representative engagements include:

- Design and implementation of ex-pat employment agreements for employees located in Iraq, Afghanistan, Africa, Central and South America, and the Caribbean
- Investigation and resolution of harassment allegations of foreign employees in Africa
- Negotiation of 70% reduction of back-pay and benefits demanded by United Mine Workers of America under the federal Worker Adjustment and Retraining Notification ("WARN") Act following shutdown of mining facility
- Design and implementation of strategic corporate diversity initiatives for company with 100,000+ employees
- Design and implementation of application and selection processes for 5,000+ management positions at Fortune 100 company
- Training of executives and senior leadership regarding talent management best practices at Fortune 100 company
- Comprehensive equity analysis of management pay at Fortune 500 company, including implementation of remedial adjustments to employee compensation

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. Representative engagements include:

- Serving as lead defense counsel in nationwide promotions class action pending before the Equal Employment Opportunity Commission (EEOC)
- Lead defense counsel in successful opposition to class certification in five putative class actions before the EEOC
- Lead defense counsel in hostile work environment and retaliatory discharge matter
- Member of defense trial team for what would have been the largest employment discrimination class action ever tried to a jury had the matter not resolved – following a significant defense victory on motions *in limine* – on the eve of trial
- Lead defense counsel for successful defense of several discrimination and wrongful termination claims filed in the District of Columbia against national hotel chain under private ADR agreement

HONORS

Recognized in the 2013 edition of *Chambers USA*, Labor & Employment, Virginia

SPEAKING ENGAGEMENTS

Mr. Warner is a frequent lecturer on topics including compliance with the McNamara-O'Hara Service Contract Act, the Davis-Bacon Act, the Family and Medical Leave Act, the Fair Labor Standards Act, reasonable accommodation under the Americans with Disabilities Act, OFCCP compliance, hiring, firing, discipline and other aspects of the employer/employee relationship touched upon by state and federal law.

VENABLE® LLP

our people

Armand J. (A.J.) Zottola

Partner

Washington, DC Office

T 202.344.8546 F 202.344.8300

ajzottola@Venable.com

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.

Mr. Zottola's skills enable him to handle all types of issues, negotiations, and agreements involving:

- intellectual property;
- franchise;
- privacy;
- information security;
- contract; and
- business tort law.

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.

REPRESENTATIVE CLIENTS

Mr. Zottola regularly represents U.S. and foreign enterprises, from *Fortune* 500 companies and small start-ups to trade and professional associations. Industries include software, e-commerce, information technology, electronics, media and entertainment, medical products, toys and other consumer products, financial services, healthcare, life sciences, telecommunications and other newer technologies.

SIGNIFICANT MATTERS

Having worked exclusively in the technology space since the beginning of the Internet age in the 1990s, Mr. Zottola has extensive experience in the areas of:

- licenses and technology transfers;
- outsourcing, professional, consulting, and Internet-enabled service arrangements;

AREAS OF PRACTICE

Technology Transactions and Outsourcing

Corporate

Privacy and Data Security

Franchise and Distribution

Advertising and Marketing Litigation

Intellectual Property Litigation

Intellectual Property Transactions

Copyrights and Licensing

Trademark Litigation

Trademarks and Brand Protection

INDUSTRIES

New Media, Media and Entertainment

Government Contractors

Life Sciences

Nonprofit Organizations and Associations

Green Businesses

BAR ADMISSIONS

Maryland

District of Columbia

EDUCATION

J.D., *cum laude*, Catholic University of America, Columbus School of Law, 1997

Editorial Assistant, *Catholic University Law Review*

Intellectual Property Summer Institute, Franklin Pierce Law Center, Concord, NH, 1995

B.A., Bucknell University, 1992

- distribution, supply, reseller, and manufacturing arrangements;
- e-commerce, information technology, data processing, and proprietary information agreements;
- strategic partnerships and alliances;
- trademark and copyright prosecution;
- technology and intellectual property due diligence;
- mergers, sales, dispositions, and acquisitions; and
- co-branding/marketing agreements, publishing agreements, and franchising agreements and networks.

Mr. Zottola has represented:

- a large technical and software services contractor in devising new open source software business models for its products and solutions;
- a large, publicly-held leader in enterprise storage management software in connection with the intellectual property aspects of acquiring a $403 million publicly held software company that provided data storage, access and e-mail management solutions;
- a large, publicly held global business and information technology company in orchestrating the intellectual property aspects of selling its global utilities practice for approximately $26 million;
- a privately held Internet entertainment and marketing business in selling all its technology assets (including its entire trademark and patent portfolio) to a large media company; and
- a large, publicly held pharmaceutical product wholesaler in connection with the intellectual property aspects of its joint venture with another public company to form an independent health informatics business.

Mr. Zottola's recent dispute resolution experience includes representing:

- a large non-profit organization in a breach of contract dispute with its data management systems provider;
- a leading children's toy company in its defense of a trademark and copyright infringement lawsuit, which also involved business tort and unfair competition claims;
- a leading scented candle manufacturer and distributor in its pursuit of trademark and copyright infringement, business tort and false advertising claims against a competitor; and
- a software company in a breach of contract dispute.

HONORS

Listed in *The Best Lawyers in America* for Technology Law (Woodward/White, Inc.), 2014

Practice ranked National Tier 1 and Washington, DC Tier 1 for Technology Law by *U.S. News-Best Lawyers "Best Law Firms,"* 2014

Recognized in the 2013 edition of *Chambers USA* (Band 3), Technology & Outsourcing, District of Columbia

Recognized in the 2012 edition of *Chambers USA* (Band 3), Technology & Outsourcing, District of Columbia

Recognized in the 2011 - 2013 editions of *Legal 500*, Technology: Outsourcing and Transactions

Additional Information

VENABLE® LLP

Articles

January 2014

Bring-Your-Own-Device Programs: Steps to Minimize Nonprofits' Legal Risks

AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr

RELATED PRACTICES

Technology Transactions and Outsourcing

Labor and Employment

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2014 2010 2006

2013 2009 2005

2012 2008 2004

2011 2007

Nonprofit organizations are increasingly allowing their employees to use their own mobile devices to access, view, download, and transmit work-related materials. While these bring-your-own-device (BYOD) programs may enhance productivity and decrease information-technology costs, these devices also can create certain legal, financial and other risks. Recent reports indicate that almost half of the employers with BYOD programs have experienced a data breach of some kind resulting from employee error or intentional wrongdoing. Even a single breach can lead to financial liability, regulatory penalties, reputational harm, and the loss or unauthorized disclosure of intellectual property. Below is a non-exhaustive list of steps to consider in connection with establishing a BYOD program or allowing employees to use their personal mobile devices for work-related activities.

BYOD Policy

First and foremost, it is important to have a written BYOD policy. Such a BYOD policy should be tailored and customized to meet the operational realities of the particular workplace. In other words, the BYOD policy should addresses all of the activities and related concerns of a particular nonprofit and not amount to a boilerplate, one-size-fits-all policy statement. When creating a BYOD policy, consider the need to address such items as trade secret protection, email/computer/system/document access or usage policies, security policies, device usage policies, sexual harassment and other equal employment opportunity matters, data breach response plans, and employee training initiatives. In addition, consider implementing the policy by obtaining informed consent to the policy statement from all BYOD program participants.

Expectations of Privacy

The use of a single device for work and personal purposes complicates efforts to monitor devices for security or investigative purposes. For instance, personal information may be accidentally deleted when devices are updated remotely, and devices may need to be searched for relevant information in the event of civil or criminal litigation, investigations or enforcement actions. Address employees' expectations of privacy in dual-use or employer-owned devices by explaining how and for what purposes their devices may be accessed or searched.

Data Security

Nonprofits that have access to, process or otherwise maintain certain types of sensitive personal information (*e.g.*, personally identifiable consumer information and nonpublic medical or financial information) must satisfy certain information security obligations imposed by rapidly evolving state and federal laws. These obligations will therefore require nonprofits to consider adequate safeguards for sensitive information that can be made accessible from mobile devices. Be familiar with what types of information must be protected and what types of information will be accessible on mobile devices, and implement the necessary procedures to satisfy applicable legal requirements.

Intellectual Property Protection

Valuable confidential information, patentable ideas, trade secrets, and/or creative works protectable by copyright law may all be accessible on a lost, stolen or intentionally misused employee device. Be sure to set forth rules relating to the use, access rights for, and retention of such information or materials on dual-use or employer-owned mobile devices.

Agency

BYOD programs may expand an employee's scope of employment by combining the workplace with the private sphere. Under certain circumstances, an employer can even be held liable for the tortious conduct or criminal behavior of its employees or the binding obligations and contracts they establish

with third parties. Clearly define what constitutes work and private use to mitigate exposure to this vicarious liability.

Employee Disability

Recent litigation has raised questions about the applicability of the Americans with Disabilities Act (ADA) to organizations engaged in electronic commerce. While the ADA does not expressly apply to BYOD programs, consider having BYOD programs that sufficiently accommodate employees with disabilities.

Labor and Employment Issues

BYOD programs may lead to disputes about overtime pay and expense reimbursement by blurring the lines between regular work hours and personal time. Moreover, BYOD programs could potentially expose a nonprofit to liability under federal and/or state law for an employee's injuries resulting from responding to work-related emails or text messages under unsafe conditions *(e.g.*, while driving a car or exercising). Consider policies for usage and also inform employees about their rights, obligations and limitations with respect to those policies.

Ongoing Effort

Following the above guidance is only the first step in mitigating risks associated with BYOD programs. Nonprofits should regularly track changes in technology, applicable laws and regulations, and workplace culture regarding dual-use devices, and consistently review, update and modify BYOD policies to address reasonably foreseeable risks and issues. And last, but certainly not least, keep employees up-to-date on BYOD issues and policies through written communication and regular training exercises.

* * * * *

Are you interested in learning more about best practices for establishing a bring-your-own-device policy for your nonprofit organization?

Join Venable partners **Armand J. (A.J.) Zottola**, **Ronald W. Taylor**, and **Jeffrey S. Tenenbaum** for a complimentary luncheon/program and webinar, **Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know**, on Wednesday, February 19, 2014. As you are now aware, BYOD policies require thoughtful and careful consideration to prevent BYOD from becoming a nonprofit's "build your own disaster." This program will provide practical guidance for nonprofits on how to reconcile the pros and cons and best practices in crafting an effective BYOD policy for your organization.

Click here for more information and to register for the event.

* * * * *

*For more information, please contact **Armand J. (A.J.) Zottola** at **ajzottola@Venable.com** or **Robert F. Parr** at **rfparr@Venable.com**.*

VENABLE® LLP

Articles

September 20, 2012

Labor Pains: Computer Hacking by Employees of Nonprofits

AUTHORS

Todd J. Horn

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

What if a former employee downloads confidential information (such as a donor or member database, fundraising strategies, new program and service plans, and the like) from your computer system and uses it to help your competitors or others? Among the laws at your disposal is the Computer Fraud and Abuse Act ("CFAA"). Although principally a criminal statute intended to combat computer hacking, the CFAA allows for a civil lawsuit against someone who obtains information from another's computer "without authorization."

Let's change the scenario slightly. What if a current employee downloads your sensitive, confidential information to his personal computer, resigns, goes to work for your arch-competitor, and then uses that information to target your donors, members, or other supporters? Do not count on the CFAA to provide a remedy for that blatant misappropriation. In *WEC Carolina Energy Solutions, LLC v. Miller*, the federal appeals court with jurisdiction over Maryland, Virginia and other mid-Atlantic states narrowly construed the CFAA in a way that does not always reach even egregious misappropriation by current employees. While the case involved a for-profit company, it is equally applicable to nonprofit employers.

In this case, Miller worked for WEC as a project director and resigned to go to work for a competitor, Arc Energy. Before he quit, Miller allegedly downloaded to his personal computer WEC's confidential information, which he used to make a presentation to a potential customer after he quit. That customer selected Arc Energy over WEC. WEC sued Miller under the CFAA for misappropriating the confidential information from its computer system. WEC established that it had a policy prohibiting employees from misusing confidential information or downloading it to a personal computer. WEC, however, did not restrict Miller's authorization to access its confidential information.

The court ruled that the CFAA was designed to target unauthorized "access" to computer information, not unauthorized "use" of that information. As a result, the court decided that the CFAA only applies when an individual "accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access." The CFAA did not apply to Miller's actions because WEC had given him authorization to access the information he took; the fact that he misused that information in violation of WEC's policies did not implicate the CFAA.

Although the court candidly noted that its decision "will likely disappoint employers hoping for a means to reign [sic] in rogue employees," the CFAA door is not completely shut to combat hacking by current employees. Depending on the content of your policies, the decision leaves room for an argument that the CFAA applies if a current employee with unrestricted computer access downloads your information for the benefit of a third party.

In this regard, in addition to standard "use and access" restrictions, computer policies should specifically emphasize that employees have no authorization to access your organization's data on behalf of outsiders. That way, if a miscreant employee who has broad computer access shares your confidential information with a third party, there may be an argument that he has exceeded the scope of his authorized access under the CFAA. The entity on whose behalf the employee obtained the information also may be on the hook for unauthorized access under an agency theory. Because the court relied on WEC's internal policies to define the contours of what constitutes "authorized" access to its computer data, nonprofit employers should review and tighten their computer use and access policies. Even if the CFAA does not apply to a particular employee's computer hacking, there are common law causes of action (such as breach of fiduciary duty and tortious interference) potentially available to provide relief. Under those causes of action as well, your computer use and access policies will play a central role.

* * * * *

*For more information, please contact Todd J. Horn at **thorn@Venable.com**. Mr. Horn is the co-author*

of Maryland Employment Law*, a book cited by courts and attorneys as a leading reference. Mr. Horn was selected as the 2011 "Lawyer of the Year" for employment law in Maryland based on peer review surveys conducted by the rating organization Best Lawyers in America. Based on client interviews,* Chambers USA *also ranked Mr. Horn in the top category in employment litigation, reporting that he "is admired as a fantastic litigator – one of the best in the courtroom, and is very professional and efficient."*

This article is not intended to provide legal advice or opinion and should not be relied on as such. Legal advice can only be provided in response to a specific fact situation.

VENABLE® LLP

Articles

March 28, 2012

Know the Risks Before You Head to the Cloud: A Primer on Cloud Computing Legal Risks and Issues for Nonprofits

AUTHORS

Armand J. (A.J.) Zottola

RELATED PRACTICES

Technology Transactions and Outsourcing

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

A "cloud" solution is generally typified by remote access to computing resources and software functionality and frequently involves the storage and maintenance of related data. Today, cloud computing facilitates applications, e-mail, peer-to-peer communication, content sharing, and electronic transactions or storage for nonprofits. In many respects, the “cloud” has become a synonym for the “Internet” as cloud computing now encompasses nearly all available computing services and resources.

Cloud offerings utlilized by nonprofits tend to come in three flavors. Infrastructure as a Service (IaaS) offerings deliver information technology infrastructure assets, such as additional computing power or storage. Platform as a Service (PaaS) offerings provide a computing platform with capabilities, such as database management, security, and workflow management, to enable end users to develop and execute their own applications. And, Software as a Service (SaaS) offerings provide software applications on a remotely accessible basis. SaaS offerings are probably the most commonly understood type of "cloud" solution.

Cloud computing solutions can avoid the traditional need to invest in computer hardware and software resources required for on-site computing power and related storage equipment and space. Costs therefore evolve from capital expenditures for information technology equipment and resources to operating expenses for the cloud providers’ fees. Cloud computing also can minimize the need for on-site, technical support service expertise that would traditionally be required to implement, maintain, and secure computer hardware and software resources. Consequently, cloud computing offers nonprofits software and storage capacity and capability without the need to invest in as much infrastructure, personnel, and software licensing.

These benefits create flexibility and potentially lower costs for the cloud customer. It is therefore not surprising that this type of computing solution has rapidly become a key component to the operation of many nonprofit organizations. Despite these potential benefits, cloud computing doesn't come without risk. Below is a list of legal risks and issues for a nonprofit to consider when procuring or using a cloud solution. These risks and issues can appear as either a contractual or an implementation issue.

Take It or Leave It. Many cloud solution agreements are non-negotiable or more favorable to the provider than the end user, which places a greater emphasis on pre-negotiation analysis in order to work around inflexible contracts.

All Services, All the Time. All computing and software providers are morphing into service providers, and this change may impact the fee structure, term length, and available warranties.

Law Is Behind the Times; Contracts Even More Important. Existing laws and governance models have not kept pace with technological development, and this may leave the contract as the only means for dispute resolution.

It's All Online. Privacy and information security concerns will only increase with cloud usage.

Less Control of Subcontractors. Cloud providers tend to use subcontractors for hosting, storage, and other related services, and these subcontractors may not be readily known or otherwise liable or responsible for performance under the agreement.

Some Things May Not Be Worth the Risk. The inherent risks associated with cloud computing may make its utilization inappropriate for mission-critical I.T. services or resources

Not Everybody is on the Same Page. Different cloud solutions on different hardware may increase the possibility of incompatibility with outside software or network systems, i.e., compatibility will be dictated by the provider and not by the customer.

Know Your SLAs. Service level agreements (SLAs) vary and may be inadequate and unchangeable.

General Outages May Be Likelier. Shared resources may increase susceptibility to a single-point of failure.

Only What You Need. The terms of a license agreement may not fit the service being offered, e.g., cloud providers may grant themselves a greater right to use a customer's data or materials than necessary to provide the cloud solution.

Own Your Data. It will be more imperative than ever to hold on to the ownership and secrecy of data and materials used with the cloud solution in order to retain rights and ensure confidential treatment.

Don't Allow a Vendor to Have Zero Responsibility. Be wary of excessive disclaimers and limits and seek the implementation of a credit or refund structure to address outages and downtime.

Am I Covered? Check available insurance policies and consider the insurance policy of the cloud provider to determine if it covers business interruption caused by vendor failure.

Know the Exits. Know how to terminate a relationship with a cloud provider and plan for how such termination will unfold in order to minimize disruption caused by transitioning to a new service provider.

Where's Your Data? Understand where a copy of all stored data is physically located.

Seek Jurisdictional Clarity. Data transfer is easy and can create jurisdictional issues because the sites where data is located or transferred and where the related services are performed or received can and will typically be different.

You Need Access to Your Data. Know how to access, audit, hold, and retrieve all data or understand the limits on such data access because regulations and e-discovery rules may mandate particular data storage, protection, and transfer protocols.

Don't Forget Compliance with Law. Regulatory compliance may extend to the cloud provider, particularly, for health, financial, educational, or children's data, and laws and regulations governing privacy and information security.

Rules Are Different Overseas. The United States has more permissive data and database rules than many other countries, particularly by comparison to Europe, where greater restrictions and rights exist.

Will It Still Be There When Disaster Strikes? Understand the cloud providers' business continuity and disaster recovery practices.

Incorporate Overall Risk Management Strategies. Cloud computing risks may expand the notion of risk from I.T. management to operational management or regulatory compliance.

Everybody Is a Renter. Limited-term software licenses will become the norm with customers not having any ownership rights in the software copy being licensed.

Courts, governmental authorities, and industry standard-setting bodies may address some of the foregoing concerns. But, until then, nonprofits considering cloud computing solutions will need to look to their written contracts as the primary vehicle to protect their rights and ensure performance. Moreover, careful due diligence of cloud providers becomes key. Nonprofits therefore should consider multiple providers and should not make decisions based purely on cost. Instead, nonprofits should seek references and involve their key decision-makers and outside advisors to assist with the procurement process in order to ensure a thorough evaluation of the potential risks and issues with cloud computing.

A.J. Zottola *is partner in Venable LLP's Technology Transactions & Outsourcing Practice, and he works regularly with the firm's nonprofit clients. For more information, contact Mr. Zottola at 202-344-8546 or* ***ajzottola@venable.com****.*

VENABLE® LLP

Articles

February 21, 2012

How Nonprofits Can Avoid the Legal Pitfalls of Telecommuting Employees

AUTHORS

Jeffrey S. Tenenbaum
David R. Warner
Nicholas M. Reiter

RELATED PRACTICES

Labor and Employment

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

As technology for the home office improves, more nonprofits and employees are taking advantage of the benefits of telecommuting. Laptops are lighter, faster, and more portable. Smartphones, iPads, and other e-readers continue to sell in record numbers. Cloud computing enhances colleagues' ability to share information efficiently. Video conferences are becoming the norm, not the exception. These technological advances, when combined with the growing concerns over gasoline prices and work-life balance, make telecommuting a very attractive option for many nonprofits and their employees.

Of course, federal and state labor laws still apply to the telecommuting employee. Whether a nonprofit should, or in some cases must, permit telecommuting depends upon an analysis of the unique issues that telecommuting raises under federal and state law. Set forth below is an overview of some of the logistical and legal issues nonprofits should consider when creating or reforming their telecommuting programs.

Which Positions Are Best Suited for Telecommuting?

No matter the technological developments, telecommuting will likely never be appropriate for every employee. For example, it is very unlikely that a nonprofit's receptionist could perform his or her duties while telecommuting. Similarly, employees performing client intake services may need to physically perform their duties at the job site. In contrast, positions which primarily entail the electronic transfer of documents or other information are typically better suited for telecommuting, subject to proper safeguards for confidentiality and client privacy. Other common characteristics of roles fit for telecommuting include a low need for direct supervision or guidance, limited face-to-face interaction, and easily measured performance benchmarks such as quantity of output instead of actual time spent at the job site.

Wage and Hour Requirements

The Fair Labor Standards Act ("FLSA") and its state law counterparts raise issues for how nonprofits monitor the work schedules of their telecommuting employees. Assuming an employee is not exempt from the overtime wage law, he or she must be paid time-and-a-half for all hours worked beyond 40 hours in a workweek. Additionally, employers are required to maintain accurate records of the hours their employees work.

Given the inherent difficulty of monitoring the work hours of a telecommuting employee, some employers offer telecommuting to exempt employees only. However, an across-the-board prohibition against telecommuting for non-exempt employees may give rise to a disparate impact claim depending upon the demographics of a nonprofit's workforce. As an alternative, many nonprofits create something akin to a virtual sign-in sheet, requiring their telecommuting employees to log-in and log-out of a web-based program at the beginning and end of their work day. Other nonprofits simply require that their telecommuting employees receive authorization from their manager prior to working beyond 8 hours in a workday or 40 hours in a workweek. However, in the event a telecommuting employee works overtime without proper authorization, the employer may not simply refuse to pay the employee overtime wages. Instead, the employer must still pay the employee overtime wages and treat the violation of the telecommuting policy as a disciplinary issue.

Occupational Safety and Health Issues

The Occupational Safety and Health Act ("OSHA") creates recordkeeping and workplace safety requirements for most employers, including many nonprofits. In contrast to the traditional work environment, the employer is typically absent when an injury to a telecommuting employee occurs. In addition, it is necessarily more difficult for an employer to monitor the safety of a telecommuting employee's workspace.

The employer's obligation to provide a safe work environment is balanced against the telecommuting employee's right to privacy in his or her home. Accordingly, an employer is not obligated to inspect a telecommuting employee's home office. However, a nonprofit's telecommuting policy should nonetheless help promote a safe home office environment. The policy should state that the telecommuting employee is responsible for ensuring that his or her workspace complies with the same safety requirements for the employer's site. The policy also should acknowledge that the telecommuting employee either has been provided equipment from the employer or has assumed responsibility for the safety of his or her own equipment.

Workers' Compensation Laws

Although the specific statutes vary among different states, workers' compensation laws generally require that an employer compensate its employees for injuries sustained in the course and scope of employment. Nonprofits may find it more difficult to ascertain whether an injury occurs in the course and scope of employment for telecommuting employees. Unlike with injuries at the employer's site, there are usually no witnesses when a telecommuting employee is injured at his or her home. In order to curb against the risk of fraudulent injury reports, the telecommuting policy should require that work-related injuries be recorded within a certain number of hours of the occurrence and that the employee make his or her home work-space available for inspection following the injury.

Implications of the Americans with Disabilities Act

The Americans with Disabilities Act ("ADA") prohibits workplace discrimination based upon an employee's disability. Assuming that an employee meets the ADA's definition of disabled, nonprofits with 15 or more employees must reasonably accommodate the employee so long as such accommodation does not result in an undue hardship for the employer. In the telecommuting context, the most critical question is whether the disabled employee can perform the essential functions of his or her job from home. Common considerations include whether: (1) the employee regularly meets with clients or customers; (2) the employee supervises other employees and/or regularly meets in person with a team of co-workers; and (3) the employee's productivity or quality of work will suffer if he or she is permitted to telecommute.

In light of these concerns, nonprofits should ensure that they have written job descriptions which clearly set forth the essential job functions of each position. As part of the interactive process, a nonprofit should refer to an employee's job description when explaining whether it permits the employee to telecommute as a reasonable accommodation. An employer is not necessarily required to permit telecommuting merely because it is the employee's preferred reasonable accommodation. In one recent case, an employee requested that she be permitted to telecommute because her disability required that she lay down periodically during the workday. Although the employer denied her request, the employer did not violate the ADA because it provided the employee with a cot in her office as an alternative reasonable accommodation for her disability.

Anti-Discrimination

Federal and state laws prohibit discrimination based upon an employee's membership in a protected class, including an employee's race, gender, national origin, religion, disability, age, and marital status, among others. In particular, telecommuting raises concerns of potential disparate impact claims. Unlike intentional forms of discrimination, disparate impact claims typically arise from a company-wide policy which adversely, albeit unintentionally, affects a disproportionate number of employees who are members of the same protected class.

For example, a nonprofit may require its telecommuting employees to dedicate an entire room in their homes as their work-space. At first glance, this policy may seem harmless. However, what if only the most affluent employees can afford to cordon an entire room in their homes for telecommuting purposes? Depending upon the socioeconomics of a nonprofit's work-force, this hypothetical telecommuting policy may disproportionately exclude members of various protected classes. In order to safeguard against a disparate impact claim, nonprofits should either allow all employees in a given position to telecommute, or alternatively, determine a number or percentage of such employees who are permitted to telecommute on a first-come, first-served basis. Nonprofits also should document all telecommuting requests and decisions so that the non-discriminatory administration of its telecommuting policy is memorialized. Finally, nonprofits must ensure that all compensation schedules and benefit programs are uniform, regardless of whether an employee telecommutes.

Medical Leave Needs

Under the Family Medical Leave Act ("FMLA"), qualified employees are permitted up to 12 weeks of leave time during any 12-month period in order to receive care for a serious health condition; to care for a spouse, child, or parent; or following the birth or adoption of a new child. An employer is subject to the FMLA's requirements so long as it employs 50 or more employees at a worksite or within 75 miles of such worksite. For telecommuting employees, their "worksite" is not their home. Rather, for purposes of the FMLA, their worksite is the office to which they report.

The most common problem arises when employers use telecommuting to pressure employees not to take medical leave. Although tempting, employers cannot require or otherwise coerce employees to telecommute in lieu of taking medical leave as permitted under the FMLA. However, employers can still offer (but not require) a reduced leave schedule with telecommuting as an option.

Privacy Issues

Telecommuting policies must balance an employee's right to privacy against the employer's need to monitor the employee's performance. Generally, a person has a valid privacy right in any matter which he or she can "reasonably expect" to remain private. Accordingly, any telecommuting policy must set forth the employee's unequivocal acknowledgment that various facets of his or her home work-site may be monitored unexpectedly, including his or her use of the employer's computer, telephone lines, or other equipment.

Protection of Confidential and Proprietary Information

Another concern telecommuting raises is the risk of unauthorized disclosure of confidential and proprietary information. Unlike work performed at the employer's work-site, there is often no way of knowing who outside the employer's organization is privy to sensitive information at the employee's home. Therefore, it is strongly recommended that any telecommuting policy include a non-disclosure agreement applicable to all information and materials used or prepared in connection with the telecommuting program. Nonprofits also should consider whether to implement stronger password and other security measures than those used at their work-sites. Furthermore, home office equipment such as computers and other devices containing work product and sensitive employer information should be dedicated for work-related activities only.

Income Taxes

Telecommuting raises tax issues where an employee telecommutes from a different state than where his or her employer is located. Although tax laws vary widely amongst the different states, income is traditionally taxable wherever it is earned. However, at least one state has departed from this norm. In 2005, New York State's highest court held that, under the state's tax law, all of an employee's wages were subject to tax in New York despite the employee having telecommuted from his home in Tennessee during 75% of the time he worked for his employer located in New York. The decision suggests that wages are "earned" wherever the employer is located unless the interstate work was performed out of necessity rather than convenience to the employee. Unfortunately, there is no blanket answer for all states, and employers must evaluate their home state's tax laws to ensure compliance.

Tort Liability

In most cases, employers bear responsibility for injuries and damage to property as a result of their employees' negligence, especially if such injury or damage occurs on the employer's property. Telecommuting asks whether the same is true for harm to a third party at an employee's home. Take, for example, the courier who slips on the snowy steps outside an employee's front door while delivering a package of work-related documents. In some cases, the employer will bear responsibility for his injuries.

In order to protect against such claims, nonprofits should make sure that their liability insurance policies cover the telecommuting employee's home when used in the course and scope of employment; be sure to consult all potentially applicable policies (e.g., commercial general liability insurance, property insurance, directors and officers liability insurance). In addition, nonprofits may require as a condition of telecommuting that employees secure liability coverage for such injuries as part of their own homeowner's or renter's insurance.

Zoning Laws

Depending upon the employee's responsibilities, applicable zoning laws and regulations may prohibit the employee from performing his essential job functions in his or her home. Many cities' zoning laws and regulations limit or restrict the operation of home businesses. In some cases, such laws and regulations will require that the employee secure a permit or license before engaging in specific work

activities within his or her home. If so, nonprofits should consider whether they or their employees will bear responsibility for securing the necessary permits or licenses.

Recommended Components of any Telecommuting Policy

In addition to the considerations outlined above, it is strongly recommended that any employer's telecommuting policy also include the following:

- A clear definition of "telecommuting" for purposes of the telecommuting policy and any related agreements between the employer and employee (*i.e.*, does telecommuting include work at home only, or does it also include other off-site locations?)
- Easy-to-understand eligibility requirements (*e.g.*, minimum length of employment and the employer's considerations for whether an employee's position is fit for telecommuting)
- The steps of the telecommuting approval procedure
- That participation in the telecommuting program is a privilege and not a right, subject to revocation at any time for any lawful reason
- That the abuse of telecommuting can result in disciplinary action, including termination of employment
- The employer's right to monitor and inspect the home work environment
- A non-disclosure and confidentiality agreement
- The employer's right to change the terms of its telecommuting policy
- That the telecommuting employee is expected to meet the same performance standards as on-site employees

---

Given the growing prevalence of telecommuting and the advances in related technology, nonprofits should look for changes in the labor and employment laws that affect telecommuting employees. As explained above, many state laws vary from both different jurisdictions and their federal counterparts. As always, it is recommended that nonprofits consult with legal counsel to ensure compliance with their specific jurisdictional requirements.

*For more information, please contact Jeff Tenenbaum at **jstenenbaum@Venable.com**, David Warner at **drwarner@Venable.com**, or Nick Reiter at **nmreiter@Venable.com**.*