A large, abstract graphic on the left side of the page, consisting of overlapping, layered shapes in shades of blue, teal, and grey, resembling a stylized arrow or a modern architectural element.

# Managing Your Nonprofit's FACEBOOK, TWITTER, and LINKEDIN Presence: Avoiding the Legal Pitfalls

Wednesday, May 13, 2015,  
12:30 – 2:00pm ET

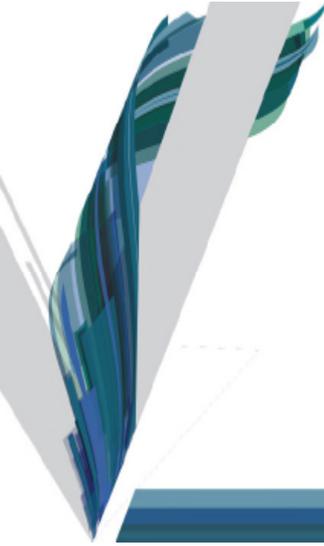
Venable LLP, Washington, DC

## **Moderator**

Jeffrey S. Tenenbaum, Esq.,  
Partner and Chair of the Nonprofit Organizations  
Practice, Venable LLP

## **Speakers**

Armand (A.J.) Zottola, Esq., Partner, Venable LLP  
Krista S. Coons, Esq., Associate, Venable LLP



# Presentation

---



## Managing Your Nonprofit's FACEBOOK, TWITTER, and LINKEDIN Presence: Avoiding the Legal Pitfalls

Wednesday, May 13, 2015, 12:30 – 2:00pm ET  
Venable LLP, Washington, DC

### Moderator

Jeffrey S. Tenenbaum, Esq., Partner and Chair of the Nonprofit Organizations Practice, Venable LLP

### Speakers

Armand (A.J.) Zottola, Esq., Partner, Venable LLP  
Krista S. Coons, Esq., Associate, Venable LLP

© 2015 Venable LLP



## CAE Credit Information

**\*Please note that CAE credit is only available to registered participants of the live program.**

As a CAE Approved Provider educational program related to the CAE exam content outline, this program may be applied for **2.5 credits** toward your CAE application or renewal professional development requirements.

*Venable LLP is a CAE Approved Provider. This program meets the requirements for fulfilling the professional development requirements to earn or maintain the Certified Association Executive credential. Every program we offer that qualifies for CAE credit will clearly identify the number of CAE credits granted for full, live participation, and we will maintain records of your participation in accordance with CAE policies. For more information about the CAE credential or Approved Provider program, please visit [www.whatiscae.org](http://www.whatiscae.org).*

*Note: This program is not endorsed, accredited, or affiliated with ASAE or the CAE Program. Applicants may use any program that meets eligibility requirements in the specific timeframe towards the exam application or renewal. There are no specific individual courses required as part of the applications—selection of eligible education is up to the applicant based on his/her needs.*

© 2015 Venable LLP

VENABLE 2



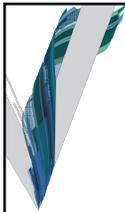
## Upcoming Venable Nonprofit Events

Register Now

- **June 4, 2015** – [Top Trends and Traps in Nonprofit Executive Compensation](#)
- **July 15, 2015** – [Mental Health Issues in the Nonprofit Workplace: Questions Raised by the Germanwings Air Disaster](#)
- **August 6, 2015** – Top Ten "Must Have" Provisions for Nonprofit Meeting Contracts (*details and registration available soon*)

© 2015 Venable LLP

VENABLE 3



## Agenda

- Introductions
- What Can Social Media Do for Your Nonprofit?
- Intellectual Property Protection and Enforcement
- Use of Content Considerations
- Social Media Management Considerations
- Other Important Platform Terms
- Questions?

© 2015 Venable LLP

VENABLE 4

## How Does Social Media Work for You?

- Promotion and advertising
- Cultivating a brand
- Community building
- Issue advocacy, grassroots lobbying
- Fundraising
- Recruitment
- Sales of products and services

*The best returns may come from diversifying across networks rather than focusing solely on the latest "it" platform, but individual strategies will vary.*



© 2015 Venable LLP

VENABLE 5

## Intellectual Property: The Basics

- **Copyright**
  - Protects creative expression fixed in any tangible or electronic medium, *e.g.*, words, designs, audio-visual content, music
- **Trademark**
  - Trademarks protect against consumer confusion by protecting indicators of source, including organization name, any logos, brands, product names, trade dress
- **Patent**
  - Protects inventive concepts
- **Trade Secret**
  - Protects information that derives independent economic value from being not known to others



© 2015 Venable LLP

VENABLE 6



## Obtaining Ownership of IP

- General rule: Organizations own IP created by their employees, but not their contractors or volunteers
  - BUT, employment status is not always clear and must be within the scope of employment
- Fix: All independent contractors and volunteers should sign a written work-made-for-hire agreement *and* copyright assignment (“belt-and-suspenders” approach)
- A “work-made-for-hire” is a work [that fits into one of nine enumerated categories and] . . . “if the parties expressly agree in . . . [writing] that the work shall be considered a work-made-for-hire”
- Assignment should cover all other subject matter, *e.g.*, webinar presentations, white papers, social media contact lists

© 2015 Venable LLP

VENABLE 7

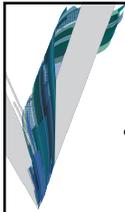


## CDM Media USA, Inc. v. Simms

- **Facts**
  - LinkedIn page contained info on private executives interested in speaking at plaintiff’s events
  - Employee went to work for a competitor and refused transfer control of the LinkedIn group, or provide the membership list and messages, to plaintiff
  - Plaintiff sued for breach of non-compete, violation of trade secret law, and misappropriation
- **Decision: Complaint Survived Motion to Dismiss**
  - Control of LinkedIn Group may constitute “Confidential Information” within meaning of the non-compete
  - Membership list might be trade secret; messages (generally) as a category are not trade secrets, but individual messages might be
  - Court dismissed claims based on breach of obligations in employee handbook because the non-compete said no other terms would govern
- **Employment, Policies, Agreements, and Procedures**
  - Employer owns all social media accounts, content, communications, and membership lists – always put these provisions in a signed writing
  - Employee must transfer accounts upon termination

© 2015 Venable LLP

VENABLE 8

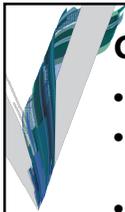


## Posting Content: Understand the Implications

- Once you share it on social media (regardless of platform), it can be shared with users who view it without limit
- Think of social media content as permanent because from a PR perspective, it is:
  - Facebook – know “delete” versus “hide” (“hide” only hides content from your Timeline while shared copies live on)
  - When you delete a tweet, it is gone
- Photos and Names/Likenesses: [Almost] always (need to) get consent from any people appearing in the photos you post to social media

© 2015 Venable LLP

VENABLE 9



## Case Study: Allowing the Unlimited Posting of Content

- Pinboard-style social media content posting
- The risk? Every time you pin (post content), the network operator copies that image to its server
- Network operators (*e.g.*, Pinterest) require through their terms of use that the entity posting content must own or have the right to post such content; the terms often include a license grant for others to re-post (among other things)
- What content can be posted or pinned?
- Pinning content from other websites also may violate a network operator’s terms of use
- How can your organization post content responsibly?
  - Safest – Only post content you own/create
  - 2<sup>nd</sup> best – Only re-post content you have a right to use
  - 3<sup>rd</sup> best – Only post from sites that have the “Pin” button installed, *i.e.*, agreed to the content sharing

© 2015 Venable LLP

VENABLE 10

## Protecting Your IP on Social Media

- Register, register, register (IP, search and account)
- May need a registration for effective copyright or trademark right enforcement
- Monitor use by others and enforce rights via policy statements, DMCA, demand letters, and legal proceedings
  - BUT, be mindful that on social media, cease and desists go VIRAL!



- Balance IP protection with reputation protection. Many times, it's an innocent infringer. Aggressive enforcement may backfire.
- Appropriate use of symbols – ©, ®, ™
- And, perhaps most importantly...Utilize network operator takedown policies and procedures

© 2015 Venable LLP

VENABLE 11

## Platform Takedown Procedures

- **Copyright infringement**
  - Generally follows Digital Millennium Copyright Act (DMCA) takedown procedures
  - Submit DMCA takedown request via online link
  - DMCA request must contain description of copyrighted work, location of infringing material, contact info, statement of good faith, and signature (e-signature)
  - Platform notifies infringer
  - If no counter-notice, content will be removed
  - Repeat infringer policies
- **Trademark infringement**
  - Submit complaint via online link
  - Submit contact info, trademark, registration info, website, location of infringing content, description of infringement
  - In some cases, complaints will result in removal of trademarked content

© 2015 Venable LLP

VENABLE 12



## Trademark Policies: Differences

- **Facebook**
  - Will provide name and contact information to the original poster
  - Will encourage original poster to reach out in the event of a dispute as to the alleged infringement
  - Otherwise, if the dispute results from an alleged infringement under U.S. law, Facebook will make ultimate determination
  - Ads have reporting feature built in (“X”)
- **Twitter**
  - Will suspend accounts if there is a clear intent to infringe
  - In unclear cases, Twitter will contact owner in an attempt to “clear up any potential confusion”
  - If the infringement is a username, Twitter may release that username to trademark owner

© 2015 Venable LLP

VENABLE 13



## Limit Apparent Authority and Protect Corporate Identity

- Limit individuals who have authority to communicate (speak) on entity’s behalf and then prohibit all others from claiming or implying authorization to (communicate) speak on entity’s behalf
  - Create process for gaining authorization to speak on entity’s behalf
- Prohibit unauthorized individuals from using entity’s intellectual property, logos, trademarks, and copyrights in any way or manner
- Prohibit employees and members from using entity’s name in any online identity (*e.g.*, username, screen name)



© 2015 Venable LLP

VENABLE 14



## Name Reservation Policies

- **Facebook – Pages**
  - Only “authorized representatives” can create a page on behalf of a brand, place, or organization
  - Users may create a page to express support for a brand or organization as long as it does not mislead or represent that it is official (disclaimer required)
- **Twitter – Handles (no pages equivalent)**
  - First come, first served basis – 15 characters maximum
  - Cannot contain the words “Twitter” or “Admin”
  - Twitter has stated that they are working to adopt automatic release of handles following infringement claims
- **LinkedIn – Company Pages**
  - Creator requirements
    - LinkedIn profile at least seven days old, with a profile strength of “Intermediate” or “All Star”
    - Current employee with position listed in profile
    - A company email address with a unique domain (e.g., no organizational Gmail account)



## Employees’ Use and Employer Rights

- Employees: Do you care what they post online?
  - Can be subpoenaed and used as evidence in a lawsuit or regulatory action
- **Tread carefully.** Terminating someone wrongfully as a result of what you they post on social media can carry stiff fines and other penalties (e.g., comments disparaging employer have been found to be protected by the NLRA)
- Do not request that your employees provide you with access to their social media pages
  - Since 2012, 20 states have enacted laws prohibiting employers from requesting such access



## Questions?

**Jeffrey S. Tenenbaum, Esq., Partner, Venable LLP**

[jstenenbaum@Venable.com](mailto:jstenenbaum@Venable.com)

t 202.344.8138

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

[ajzottola@Venable.com](mailto:ajzottola@Venable.com)

t 202.344.8546

**Krista S. Coons, Esq., Associate, Venable LLP**

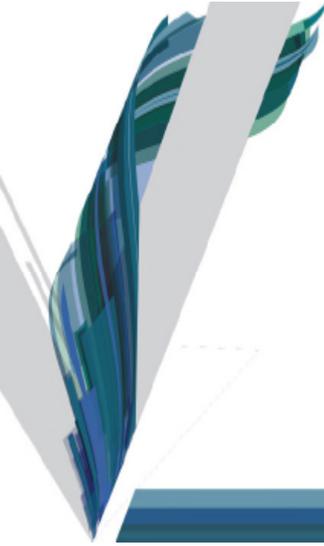
[kscoons@Venable.com](mailto:kscoons@Venable.com)

t 212.503.0552

t 415.653.3750

To view an index of Venable's articles and presentations or upcoming programs on nonprofit legal topics, see [www.Venable.com/nonprofits/publications](http://www.Venable.com/nonprofits/publications) or [www.Venable.com/nonprofits/events](http://www.Venable.com/nonprofits/events).

To view recordings of Venable's nonprofit programs on our YouTube channel, see [www.youtube.com/user/VenableNonprofits](http://www.youtube.com/user/VenableNonprofits) or [www.Venable.com/nonprofits/recordings](http://www.Venable.com/nonprofits/recordings).



# Speaker Biographies

---



## Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

[jstenenbaum@Venable.com](mailto:jstenenbaum@Venable.com)

### 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  
 Financial Services

### GOVERNMENT EXPERIENCE

Legislative Aide, United States House of Representatives

### BAR ADMISSIONS

District of Columbia

### EDUCATION

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

Jeffrey Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. He is one of the nation's leading nonprofit attorneys, and also is a highly 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, one of only eight in the 2013 rankings, and one of only nine in the 2014 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 2015 recipient of the New York Society of Association Executives' Outstanding Associate Member Award, 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 2012-15 editions of *The Best Lawyers in America* for Non-Profit/Charities Law, and was selected for inclusion in the 2014 and 2015 editions of *Washington DC Super Lawyers* in the Nonprofit Organizations category. In 2011, he was named as one of Washington, DC's "Legal Elite" 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.

### REPRESENTATIVE CLIENTS

AARP  
 Air Conditioning Contractors of America  
 Airlines for 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 Friends of Yahad in Unum

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

## MEMBERSHIPS

American Society of Association Executives

New York Society of Association Executives

American Institute of Architects  
American Institute of Certified Public Accountants  
American Society for Microbiology  
American Society of Anesthesiologists  
American Society of Association Executives  
America's Health Insurance Plans  
Association for Healthcare Philanthropy  
Association for Talent Development  
Association of Clinical Research Professionals  
Association of Corporate Counsel  
Association of Fundraising Professionals  
Association of Global Automakers  
Association of Private Sector Colleges and Universities  
Auto Care Association  
Biotechnology Industry Organization  
Brookings Institution  
Carbon War Room  
The College Board  
CompTIA  
Council on Foundations  
CropLife America  
Cruise Lines International Association  
Design-Build Institute of America  
Endocrine Society  
Ethics Resource Center  
Foundation for the Malcolm Baldrige National Quality Award  
Gerontological Society of America  
Global Impact  
Goodwill Industries International  
Graduate Management Admission Council  
Habitat for Humanity International  
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  
March of Dimes  
ment'or BKB Foundation  
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 Manufacturers  
National Association of Music Merchants  
National Athletic Trainers' Association  
National Board of Medical Examiners  
National Coalition for Cancer Survivorship  
National Council of Architectural Registration Boards  
National Defense Industrial Association  
National Fallen Firefighters Foundation  
National Fish and Wildlife Foundation  
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  
Telecommunications Industry Association  
Trust for Architectural Easements  
The Tyra Banks TZONE Foundation  
U.S. Chamber of Commerce  
United Nations High Commissioner for Refugees  
United States Tennis Association  
University of California  
Volunteers of America  
Water Environment Federation

## HONORS

Recipient, New York Society of Association Executives' Outstanding Associate Member Award, 2015

Recognized as "Leading Lawyer" in *Legal 500*, Not-For-Profit, 2012-14

Listed in *The Best Lawyers in America* for Non-Profit/Charities Law, Washington, DC (Woodward/White, Inc.), 2012-15

Selected for inclusion in *Washington DC Super Lawyers*, Nonprofit Organizations, 2014-15

Served as member of the selection panel for the inaugural *CEO Update* Association Leadership Awards, 2014

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 700 articles.

## SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer on nonprofit legal topics, having delivered over 700 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.



## Armand J. (A.J.) Zottola

Partner

Washington, DC Office

T 202.344.8546 F 202.344.8300

[ajzottola@Venable.com](mailto:ajzottola@Venable.com)

### 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

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;

## 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 and 2015

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 *Chambers USA* (Band 3), Technology & Outsourcing, District of Columbia, 2012 - 2014

Recognized in the 2011 - 2014 editions of *Legal 500*, Technology: Outsourcing and Transactions

## PUBLICATIONS

- May 4, 2015, Essential Steps to Consider When Your Company Becomes the Target of a Phishing Scam, *Digital Rights Review*
- March 25, 2015, Apps Apps Everywhere: 5 Essential Legal Considerations for Companies Developing a Mobile App, *Electronic Retailing Association's (ERA) Blog*
- March 2015, *Association TRENDS* 2015 Legal Review
- 2014 and 2015, United States chapter, *Getting the Deal Through – Outsourcing 2014* and publication update for 2015

- February 2015, Digital Media Link - February 4, 2015, Digital Media Link
- January 2015, Enforceability of Online Terms of Use: Guidance from the Ninth Circuit, *The Licensing Journal*
- December 15, 2014, Enforceability of Online Terms of Use: Guidance for Nonprofits from a Federal Appeals Court
- December 12, 2014, 10 Steps To A FINRA-Compliant Social Media Policy, *Law360*
- December 11, 2014, Advertising Law News & Analysis - December 11, 2014, Advertising Alert
- November 2014, Ten Practical Tips for Developing a FINRA-Compliant Social Media Policy, Client Alerts
- November 2014, Enforceability of Online Terms of Use: Guidance from the Ninth Circuit, Digital Media Link
- November 13, 2014, Advertising Law News & Analysis - November 13, 2014, Advertising Alert
- October 2014, A Marketplace for Ideas: 5 Things Companies Should Know About the New IP Financial Exchange, Client Alerts
- October 24, 2014, Five Vital Legal Considerations for Nonprofits Developing a Mobile App
- October 14, 2014, 5 Essential Legal Considerations For Cos. Developing Apps, *Law360*
- October, 2014, Digital Rights Review: Summer/Fall 2014 Federal Copyright and Trade Secret Legislation Update
- October 7, 2014, Nonprofits and Intellectual Property: What Every State Regulator Needs to Know
- October, 2014, Apps Apps Everywhere: 5 Essential Legal Considerations for Companies Developing a Mobile App, IP Buzz
- October 2014, United States chapter, *Getting the Deal Through – Outsourcing 2014*
- July/August 2014, If You've Got a BYOD Policy, You've Got Legal Risks
- Spring 2014, Guidelines for Protecting Company Trade Secrets, *Employers and the Law: 2013-14 Anthology of Best Articles*
- April 30, 2014, Considerations for Businesses When Using Getty's New "Free" Images
- April 23, 2014, Considerations for Nonprofits when Using Getty's New "Free" Images
- April 2014, Legal Considerations for E-Commerce Businesses, Client Alerts
- April 3, 2014, BYOD for 501(c)s: Pros and Perils of "Bring Your Own Device"
- February 2014, Winter 2014 Federal Copyright and Trade Secret Legislation Update
- February 19, 2014, Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know
- February 3, 2014, Bring-Your-Own-Device Programs: Steps to Minimize Nonprofits' Legal Risks
- January 2014, Guidelines for Negotiating Online Advertising Arrangements, *The Licensing Journal*
- November 5, 2013, Guidelines for Nonprofits when Negotiating Online Advertising Arrangements
- November 1, 2013, Advertising News & Analysis - November 1, 2013, Advertising Alert
- October 2013, Guidelines for Negotiating Online Advertising Arrangements, Technology Transactions Alert
- September 2013, Allowing User-Generated Content on Social Media: Steps for Minimizing Nonprofits' Legal Risks
- September 27, 2013, Building and Protecting Your Association's Brand in Social Media: Managing the Legal Pitfalls
- September 26, 2013, Nonprofit Executive Summit: Bringing Nonprofit Leaders Together to Discuss Legal, Finance, Tax, and Operational Issues Impacting the

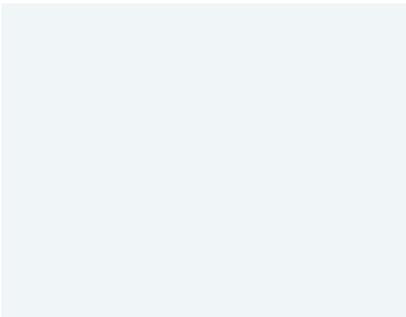
## Sector

- September 18, 2013, Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting
- June 13, 2013, Advertising News & Analysis - June 13, 2013, Advertising Alert
- May 2013, Guidelines for Protecting Company Trade Secrets, *Employers and the Law: 2013-14 Anthology of Best Articles*, Technology Transactions Alert
- April 2013, Information Security Implications for Business Agreements, Technology Transactions Alert
- April 9, 2013, Legal Risks for Associations in Social Media
- March 13, 2013, Preparing an Online Social Media Policy: The Top Ten Legal Considerations for Your Nonprofit
- January 2013, Trade Secret Legislation May Increase Infringement Claims and Lead to a Private Right of Action, Technology Transactions Alert
- December 20, 2012, Guidelines for Nonprofits for Creating Enforceable Contracts Online
- December 20, 2012, Guidelines for Creating Enforceable Contracts Online – The New Way is the Same as the Old Way, *Association of Corporate Counsel*
- December 11, 2012, Understanding the Dark Sides of the Cloud: Top Ten Legal Risks for Cloud Computing Users, *Association of Corporate Counsel*
- December 11, 2012, Understanding the Dark Sides of the Cloud: Top Ten Legal Risks for Cloud Computing Providers, *Association of Corporate Counsel*
- September 2012, Contracts 2.0: Making and Enforcing Contracts Online
- July 2, 2012, Online Social Media Legal Risks for Associations
- June 13, 2012, Ten Best Practices for Protecting Your Nonprofit's Intellectual Property
- April 26, 2012, Social Media and Charitable Solicitation Considerations
- March 28, 2012, Know the Risks Before You Head to the Cloud: A Primer on Cloud Computing Legal Risks and Issues for Nonprofits
- January 2012, Enforcing Non-Compete Provisions in California, Labor & Employment News Alert
- September 19, 2011, Does Twitter Content Require Permission to Use?, *Association Media & Publishing*
- May 19, 2011, Online Social Media and Nonprofits: Navigating the Legal Pitfalls
- January 11, 2011, The Top Five Technology Legal Traps for the Unwary Nonprofit Organization
- December 16, 2010, So You Want To Be On The Internet<sup>®</sup>
- October 5, 2010, The Top Five Technology Legal Traps for the Unwary Association
- June 24, 2010, The Legal Aspects of Social Media: What Every Association Needs to Know
- March 2, 2010, Social Media: Opportunities and Legal Pitfalls
- February 2010, Handling Unsolicited Idea Submissions, Technology Transactions Alert
- November 20, 2009, A Checklist for Social Media Legal Notices and Policies
- October 12, 2009, The Legal Aspects of Online Social Networks: An Overview for Associations
- July 2009, Electronic Health Records: "Meaningful Use" in a Land Rush, Healthcare Alert
- April 27, 2009, New Government Grants to Spur Green Technology Development, Technology Transactions Alert
- March 2009, Author, "Ways in Which an Intellectual Property Professional Can Use the World Wide Web & Gopher Servers on the Internet", *Franklin Pierce Law Center Web site*
- March 2009, Co-Author, "Avoiding Intellectual Property Law Liability", *PLI Paper*,

- November 2008, Co-author, "Clawing Your Way to the Top: Avoid SEO Liability", *Electronic Retailer Magazine*, Vol. 5, No. 11

## SPEAKING ENGAGEMENTS

- May 13, 2015, Managing Your Nonprofit's FACEBOOK, TWITTER, and LINKEDIN Presence: Avoiding the Legal Pitfalls
- February 5, 2015, "Intellectual Property of Nonprofits – Perspectives and Intersections" for the Columbia Law School National State Attorneys General Program – Charities Regulation and Oversight Project
- October 7, 2014, "Nonprofits and Intellectual Property: What Every State Regulator Needs to Know" at the 2014 National Association of Attorneys General/National Association of State Charity Officials Conference
- April 3, 2014, *Association TRENDS* Webinar: "BYOD for 501(c)s: Pros and Perils of 'Bring Your Own Device'"
- February 19, 2014, Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know
- December 12, 2013, "Making Nice with Bring Your Own Device - Tips for Successfully Implementing a BYOD Policy," WMACCA Technology and IP Forum
- September 27, 2013, "Building and Protecting Your Association's Brand in Social Media: Managing the Legal Pitfalls" at ASAE's Annual Association Law Symposium
- September 26, 2013, Nonprofit Executive Summit: Bringing Nonprofit Leaders Together to Discuss Legal, Finance, Tax, and Operational Issues Impacting the Sector
- September 18, 2013, Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting
- May 20, 2013, "Keeping Your Website Out of Legal Hot Water" for Nonprofit Spark Radio
- May 2, 2013, "Online Social Media Legal Risks for Associations" for the RAFFA Learning Community
- April 17, 2013, Government Contracts Symposium
- March 13, 2013, Preparing an Online Social Media Policy: The Top Ten Legal Considerations for Your Nonprofit
- October 26, 2012, "Online Social Media Legal Issues and Risks" at TRENDS Communications LIVE: Annual Legal Update
- September 30, 2012 - October 3, 2012, Association of Corporate Counsel (ACC) 2012 Annual Meeting
- June 13, 2012, Ten Best Practices for Protecting Your Nonprofit's Intellectual Property
- May 17, 2012, "Key Legal Issues to Consider When Procuring Cloud Computing Solutions" for Licensing Executives Society
- April 26, 2012, "Social Media and Charitable Solicitation Considerations" at the 2012 Exempt Organizations General Counsel Conference
- February 2, 2012, "SOPA, PIPA and the MEGAUPLOAD Indictment: What Do these Developments Mean for the Internet?" for the Association of Corporate Counsel's IT, Privacy & eCommerce Committee
- September 1, 2011, "Cloud Computing Legal Issues" for the Association of Corporate Counsel's IT, Privacy & eCommerce Committee
- May 19, 2011, Association of Corporate Counsel Webcast: "Online Social Media and Nonprofits: Navigating the Legal Pitfalls"
- January 11, 2011, Legal Quick Hit: "The Top Five Technology Legal Traps for the Unwary Nonprofit" for the Association of Corporate Counsel's Nonprofit Organizations Committee
- August 4, 2010, "Avoiding Legal Pitfalls When Using On-Line Social Media" for the



Indiana Grantmakers Alliance, in collaboration with various State Grantmakers Alliances

- June 24, 2010, "The Legal Aspects of Social Media: What Every Association Needs to Know," Higher Logic's 2010 Learning Series
- March 2, 2010, "Legal Aspects of Social Media" at the SocialLex Conference 2010
- June 5, 2006 - June 6, 2006, 2006 Finance & Business Operations Symposium
- August 1998, "Are you Ready? What Every Nonprofit Should Know and Do About Year 2000 – Legal Implications, Preparations, and Practical Actions," at a program hosted by Gifts In Kind International



## Krista S. Coons

Associate

*New York, NY Office  
San Francisco, CA Office*

T 212.503.0552 F 212.307.5598  
415.653.3750 415.653.3755

[kscoons@Venable.com](mailto:kscoons@Venable.com)

### AREAS OF PRACTICE

Corporate  
Technology Transactions and Outsourcing  
Copyrights and Licensing  
Intellectual Property  
Intellectual Property Litigation  
Brand Protection  
Trademarks and Brand Protection  
Domain Names and Cyber Protection  
Intellectual Property Transactions

### INDUSTRIES

New Media, Media and Entertainment  
Entertainment Industry Professionals  
Digital Media



*Digital Media Link Newsletter*

### BAR ADMISSIONS

New York

Krista Sirola Coons's practice focuses on digital media, intellectual property and technology transactions. Her experience includes drafting and negotiating major digital marketing and promotional partnerships, including: sponsorship and other talent agreements; content production and distribution agreements; live performance agreements; co-branding and other strategic alliance agreements, and agency agreements. Ms. Coons also counsels clients, generally, on the development of advertising and marketing programs as those programs relate to intellectual property rights, entertainment issues and social media, among other things.

In addition, Ms. Coons structures and negotiates various other intellectual property and technology agreements, including distribution, licensing, software development, hosting and services agreements. She also counsels clients on a range of intellectual property issues, including registration, clearance, rights of publicity, trade secrets, domain name registration and use, website terms of use, use of social media and data protection and privacy. She has experience litigating intellectual property disputes concerning issues such as trademark prosecution and infringement, copyright infringement and the Digital Millennium Copyright Act (DMCA).

Ms. Coons's clients range from Fortune 100 companies to start-ups, and represent a wide range of sectors, including the financial services, consumer goods, technology and media industries.

Prior to joining Venable, Ms. Coons was Content Protection Counsel for the Motion Picture Association of America, Inc. (MPAA), where she coordinated copyright and trademark enforcement efforts worldwide on behalf of the six major motion picture studios, which included developing and implementing legal strategy, managing content protection litigation and outside counsel and negotiating technology-related vendor and website agreements. She also provided legal guidance and support to the MPAA's member studios and content protection operations worldwide on issues such as copyright infringement, the DMCA, anti-counterfeiting statutes, cybersquatting, investigative practices, data protection and privacy and other related issues. She began her career as an associate in the Intellectual Property and Technology Practice of a major international law firm.

### PUBLICATIONS

- 2014, United States chapter, *Getting the Deal Through – Outsourcing 2014*
- September 18, 2013, Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting
- June 25, 2013, Social Media Legal Risks for Nonprofits: How to Successfully Navigate the Pitfalls
- April 9, 2013, So You Want to Create an App?: Important Legal Considerations for

California

## EDUCATION

J.D., *cum laude*, American University, Washington College of Law, 2006

Editor-in-Chief, *American University Journal of Gender, Social Policy & the Law*

B.A., Political Science and History, UCLA, 2000

## MEMBERSHIPS

American Bar Association,  
Intellectual Property Section  
Copyright Society of the U.S.A.  
California Bar and New York Bar,  
Intellectual Property Section

Nonprofits

- March 28, 2013, *Kirtsaeng v. John Wiley & Sons, Inc.*: Supreme Court Holds that the First Sale Doctrine Applies Regardless of Where a Work is Manufactured, IP Buzz
- February 26, 2013, *Kirtsaeng v. John Wiley & Sons, Inc.*: A Brief History of a Long-Anticipated Case, IP Buzz

## SPEAKING ENGAGEMENTS

- May 13, 2015, Managing Your Nonprofit's FACEBOOK, TWITTER, and LINKEDIN Presence: Avoiding the Legal Pitfalls
- September 18, 2013, Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting
- June 25, 2013, "Social Media Legal Risks for Nonprofits: How to Successfully Navigate the Pitfalls" for a New York Society of Association Executives Law SIG Luncheon
- April 9, 2013, Legal Quick Hit: "So You Want to Create an App?: Important Legal Considerations for Nonprofits" for the Association of Corporate Counsel's Nonprofit Organizations Committee



# Additional Information

---

## ARTICLES

December 15, 2014

### ENFORCEABILITY OF ONLINE TERMS OF USE: GUIDANCE FOR NONPROFITS FROM A FEDERAL APPEALS COURT

#### AUTHORS

Armand J. (A.J.) Zottola  
Jeffrey S. Tenenbaum

#### RELATED PRACTICES

Technology Transactions  
and Outsourcing

#### RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

#### ARCHIVES

2015 2011 2007  
2014 2010 2006  
2013 2009 2005  
2012 2008

The U.S. Court of Appeals for the Ninth Circuit recently decided a case addressing the enforceability of "browsewrap" terms of use, which are terms posted on websites as mere notices that are not affirmatively accepted by users through a formal acceptance process such as checking an "I agree" box. This case reinforces certain principles of online contract formation and provides helpful guidance to nonprofits of all types and sizes that use websites and/or mobile applications to facilitate their communication, marketing, fundraising, and other efforts.

#### Background

In a recent decision, *Nguyen v. Barnes & Noble Inc.*, 2014 U.S. App. LEXIS 15868 (9th Cir. August 18, 2014), the plaintiff alleged that the website operator engaged in deceptive business practices and false advertising by cancelling an order placed through the website operator's website. The website operator moved to compel arbitration because the terms of use (TOU) posted on its website contained a provision that required all disputes arising out of website use to be resolved through arbitration. The plaintiff argued that it was not bound by this arbitration provision because it neither had notice of, nor agreed to, the TOU. In response, the website operator argued that the arbitration provision was enforceable because (i) the placement of the TOU on the website provided constructive notice of the contract, including its arbitration provisions; and (ii) the plaintiff continued to use the website after such notice.

In analyzing the case, the court closely scrutinized the website's actual design and content, as well as the contract notice and implementation measures used for the TOU. Following this review, the court concluded that (i) the TOU was accessible through underlined hyperlinks set in green typeface located in the bottom left-hand corner of every page on the website; and (ii) those hyperlinks were located (a) alongside other legal notices, and (b) in proximity to buttons users must click to complete online purchases. Despite these findings, the Ninth Circuit Court of Appeals ultimately ruled against the website operator as follows:

"[W]here a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on – without more – is insufficient to give rise to constructive notice."

Accordingly, the court held that the plaintiff did not receive sufficient notice of the TOU, and therefore did not accept the terms and enter into a contract with the website operator. Without an enforceable contract, the website operator could not rely upon arbitration as a means to address the plaintiff's claims.

#### Implications

This recent decision does not break any new legal ground. Traditional contract formation analysis will still apply to website terms of use. Nonetheless, this case does illustrate and confirm a number of important principles that bear repeating about the use and enforceability of online contracts. For instance, courts remain reluctant to enforce against individual consumers normally bargained-for contractual terms contained in browsewrap agreements, including, without limitation, forum selection clauses, class action waivers, and/or mandatory arbitration provisions. In addition, this decision highlights the importance of evaluating the unique facts and circumstances when considering whether to implement terms of use through a browsewrap agreement or a more formal clickwrap agreement (*i.e.*, terms that must be accepted through some affirmative process). The content and functionality of the

website, the website operator's risk tolerance, the products and services offered on the website, the particular terms included in the terms of use, whether any fees apply, and the types of contracting parties and their respective bargaining positions can all be relevant in determining the proper method for implementing terms of use under the applicable circumstances.

Furthermore, this decision teaches nonprofits not to lose sight of the vital fact that drafting properly customized terms of use for a particular website is only half the battle. All online legal terms also must be presented to and implemented with users in a manner that would make them enforceable. Otherwise, even the most protective and clearly drafted terms of use are at risk of being set aside.

Lastly, although this case does not directly address principles of online contract formation on mobile applications, it seems to suggest that nonprofits should be particularly cautious when considering how to implement online agreements on mobile applications.

## ARTICLES

April 23, 2014

### CONSIDERATIONS FOR NONPROFITS WHEN USING GETTY'S NEW "FREE" IMAGES

*This article was also published in the May/June 2014 edition of Signature magazine and in a National Association of Home Builders e-newsletter on May 2, 2014.*

---

## AUTHORS

Armand J. (A.J.) Zottola  
Morgan E. Brubaker

## RELATED PRACTICES

Copyrights and Licensing

## RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

## ARCHIVES

2015 2011 2007  
2014 2010 2006  
2013 2009 2005  
2012 2008

Getty Images, one of the largest online U.S. stock photo image companies, recently made over 35 million photo images from its inventory available for free online use by any interested person. Getty had previously charged for the use of all of its images. Given the ease with which a digital image can be copied, however, frequent use of Getty's images online caused the images to turn up in search engine results that led to rampant re-use and sharing by additional persons without an appropriate legal license from Getty. This shift in Getty's policy offers a new approach to prior and often unsuccessful attempts by Getty to control the systemic infringement of its images online. Getty's new policy provides a select group of images for free via a new embedding feature that provides attribution and a link back to Getty Images' website. Beginning March 6, 2014, a nonprofit entity will be able to visit Getty Images' library of content, select an image, and copy an HTML-embedded code to use the image on its own website.

Nonprofits often make frequent use of Getty images on their respective websites. This policy shift offers an intriguing option for nonprofits to exploit a Getty image at no cost. Although nonprofit organizations can use these photos for free, it remains critical to understand the limits of Getty's new policy.

The new Getty policy does not permit all types of use. Specifically, Getty Images' Terms of Service states that the images cannot be used: "...for any commercial purpose (for example, in advertising, promotions or merchandising) or to suggest endorsement or sponsorship." The line between what kind of use constitutes commercial use as opposed to non-commercial use on the Internet is murky at best. Consequently, understanding the limits of Getty's free usage option may prove difficult to navigate. Getty has yet to offer a comprehensive interpretation of its Terms of Service for this new image policy.

Some pieces of insight from Getty on its interpretation of what constitutes "commercial purposes" have begun to emerge. In a recent statement emailed to the online publication GeekWire, a Getty spokesperson said the following:

*"Embedded Getty Images content may be used only for editorial, non-commercial purposes (meaning relating to events that are newsworthy or of public interest). If the use promotes a company, product, or service, the users will need to purchase a license. If not, they can use the embedded content so long as they are happy to use it in the embed frame and functionality. The presence of ads on a site doesn't automatically make use of an embedded image on that site a commercial use. Think about sites like CNN.com or any online newspapers or magazines which support editorial content with site ads. The key attribute in classifying use as commercial is whether the image is used to promote a business, goods or services, or to advertise something. If not, it is a non-commercial use. Likewise, corporate blogs would be treated as editorial/non-commercial unless the image is directly being used to sell or promote their products or services."*

This recent statement helps to clarify Getty's own interpretation. First, it is now clear that nonprofit entities likely cannot use the images to market their own products or services. Further, it is likewise clear that use in connection with editorial or news-based activities looks acceptable. But, use generally on a website, in connection with programs or events, or where other third-party advertising is a part of the use remains less clear. In other words, grey areas remain.

Nonprofit entities should keep another issue in mind when determining whether to use the free images.

According to Getty's Terms of Service, Getty gives to itself some additional rights in connection with providing the photos at no cost, namely, "Getty Images (or third parties acting on its behalf) may collect data related to use of the Embedded Viewer and embedded Getty Images Content, and reserves the right to place advertisements in the Embedded Viewer or otherwise monetize its use without any compensation to you." The data collection may relate to benign purposes. However, the opportunity exists for targeted advertising over which a nonprofit may not be in a position to exert much control. Accordingly, use of a free image may require allowance for uncontrolled third-party images and advertisements.

Overall, while the release of these photos by Getty is certainly a great opportunity for the enhancement of web content for nonprofits with limited budgets, it is important to use the images with caution. Nonprofit entities should keep in mind the restrictions on use as well as the possibility of the placement of future ads when determining how and where to use the new free images.

## ARTICLES

October 24, 2014

### FIVE VITAL LEGAL CONSIDERATIONS FOR NONPROFITS DEVELOPING A MOBILE APP

Mobile applications or "apps" are everywhere. Mobile devices are outselling personal computers, and an increasing percentage of internet access is made through mobile devices. These developments have driven the rapidly growing usage of apps. It has, therefore, become increasingly important for nonprofit organizations to invest in and develop mobile apps. Because mobile apps are essentially just a specific type of software, app development presents many of the same challenges involved in a traditional software development project. However, there are some pronounced and unique intellectual property, ownership, privacy, data security, and advertising considerations that every nonprofit should keep in mind when developing a mobile app.

#### Intellectual Property Considerations

Intellectual property considerations encompass a large and extremely important aspect of building an app. Generally, apps may contain trademark rights with respect to identifying the app, related services, or the nonprofit; copyrightable content, including the code used to build the app; trade secret rights with respect to the functionality and development of the app; and, in some circumstances, an app may even contain patentable subject matter. Retaining these rights in an app may require further action to ensure that the various parts of the app are properly protected.

#### Work-for-Hire Arrangements

In order to assert any intellectual property rights in an app in the first place, a nonprofit should ensure that any contractors or third parties who assist in the development of the app (even if such development is done on a cost-free or volunteer basis by a contractor or third party) sign a work-for-hire agreement or that their contracts contain a work-for-hire provision. A **"work made for hire"** is a work specially ordered or commissioned [if it fits into one of nine enumerated categories]...if the parties expressly agree in a written instrument signed by them that the work shall be considered a "work made for hire." While a nonprofit may obtain intellectual property rights in an app if it is created by an employee within the scope of their employment, for greater certainty, nonprofits should consider a signed agreement by which the employee-developer assigns all intellectual property rights in the app to the employer. Generally, without a work-for-hire agreement, the developer who writes the app may have a claim of copyright (or patent) in the app.

#### Distribution Considerations

Once an app is built, nonprofits should consider how to disseminate the app to the target audience and to inform others that the app is available for downloading and use. Consider whether the app will be available for free or for a fee, which could create additional obligations to facilitate the payment process. Consider further which app stores and mobile platforms will provide the opportunity and the right to distribute an app. Some platform providers are more prescriptive than others, and the agreements required by app stores and platforms vary in complexity. The agreements offered by app stores and platform providers (e.g., Apple's iOS Developer Program License Agreement or Google's Google Play Developer Program Policies for Android devices) often seek to incorporate various additional usage or compliance policies that may have consequences to the development and distribution of the app. Additionally, platforms and app stores often require certain amounts of insurance for liability coverage and likely will reserve their right to change or alter their terms at any time and are therefore free to introduce additional requirements. The app must comply with such conditions at all times, as failing to do so has the potential to give rise to legal action and/or the removal of the app from the platform.

#### Privacy and Data Security

Privacy laws and compliance have become a primary area of concern in mobile app development and implementation. Privacy issues and regulations generally revolve around the following issues:

## AUTHORS

Armand J. (A.J.) Zottola  
Morgan E. Brubaker  
Jeffrey S. Tenenbaum

## RELATED PRACTICES

Corporate  
Technology Transactions and Outsourcing  
Copyrights and Licensing  
Intellectual Property  
Intellectual Property Litigation  
Brand Protection  
Trademarks and Brand Protection  
Domain Names and Cyber Protection

## RELATED INDUSTRIES

Nonprofit Organizations and Associations

## ARCHIVES

2015 2011 2007  
2014 2010 2006  
2013 2009 2005  
2012 2008

- The kind of personal information being collected;
- The type of collection;
- The subject of the collection, and whether such subject is under the age of 13;
- The need for and ability to comply with an opt-in or opt-out mechanism;
- The country of origin or residency of end users;
- The freedoms or restrictions on use of the collected data; and
- The requirement to provide notice and a summary of data collection and use practices.

While all personal information must be protected to some degree, the collection of protected health information (PHI) and financial and credit card information (PCI) is uniquely regulated, as is collecting information from children under the age of 13 or even under the age of 18 (or other legal age of majority). Additionally, unlike traditional software applications, mobile apps may collect technical information, such as IP addresses, geo-location, and other transaction data that may be considered personal information and subject to privacy and other regulations which may vary by state and country and are constantly evolving. Some state laws specifically require the posting of a privacy policy within the mobile app if any type of personal or credit card information is collected via download or operation of the app. Privacy policies can be monitored by governmental agencies and third parties for accuracy. Non-compliance or inaccuracy can be considered a deceptive trade practice that can lead to fines and other consequences from the Federal Trade Commission and/or state Attorneys General.

### **Advertising Considerations**

Marketing or selling an app subjects a nonprofit to additional laws and regulations governing advertising. Certain solicitation efforts may require additional compliance with laws governing outreach or communication with end users. Contests and sweepstakes offered through an app likewise require additional compliance. Potential advertising issues require particular consideration when building the functionality of a mobile app.

For example, all communications sent through or in connection with a mobile app can require additional compliance actions with the Telephone Consumer Protection Act and related Federal Communications Commission rules. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) rules regulate certain commercial email and text message communications to consumers. Additionally, many state laws exist that regulate commercial text messages. The Federal Trade Commission's Truth-in-Advertising laws additionally require that all information about the app be truthful and complete, and that any objective statements about the app be backed with evidence. Other state-specific laws, and the laws of foreign countries, can apply.

Overall, app development can bring great opportunity, visibility, and income to a nonprofit organization. Nonprofits, however, should consider the significant issues associated with development, marketing, licensing, and distribution of an app in order to avoid potential liability risks.

## CLIENT ALERTS

### AUTHORS

Armand J. (A.J.) Zottola

### RELATED PRACTICES

Intellectual Property

Intellectual Property

Transactions

### ARCHIVES

2015 2011 2007

2014 2010 2006

2013 2009 2005

2012 2008

April 2014

### LEGAL CONSIDERATIONS FOR E-COMMERCE BUSINESSES

Nearly all companies now use online or mobile websites and/or social media network pages to promote their businesses, sell goods or services, conduct business transactions, and connect and communicate with customers, clients, or other businesses. While these "e-commerce businesses" confront a variety of the same legal issues faced by traditional brick-and-mortar companies, they also must manage other challenges that are unique to conducting business operations and transactions in an electronic environment. The range of legal issues to consider and manage continues to grow, and ignoring this reality could lead to financial liability, regulatory penalties, or unauthorized exploitation of company intellectual property. Set forth below is a non-exhaustive list of potential legal issues to consider in connection with minimizing the risks associated with operating an e-commerce business.

#### **Consider Agreements with Online Service Providers**

Negotiate carefully all written agreements with contractors that provide website design, hosting, advertisement, or other related online services. Consider the use of provisions that address intellectual property ownership, third-party rights clearance, information security and confidentiality, and search engine optimization practices.

#### **Consider Domain Name Selection**

Consider carefully any third-party trademark rights that may attach to a particular URL in order to avoid using a domain name that violates third-party trademark rights.

#### **Protect Website Content**

Protect content and materials appearing on proprietary websites or social media pages from unauthorized commercial exploitation by users. Consider using a <sup>TM</sup>, <sup>®</sup>, and/or <sup>©</sup> symbol in connection with prominent placements of trademarks and copyrights and register important intellectual property with the applicable authorities to perfect ownership and obtain enhanced rights and remedies. In addition, provide notices and conditions for any use or display of the intellectual property by third parties, and review publishable material before display or launch to ensure that no confidential proprietary information has been inadvertently disclosed.

#### **Create Enforceable Online Contracts**

Traditional contract principles apply to transactions conducted online. This means that each online contract requires an offer, acceptance, and consideration (i.e., a bargained-for exchange of detriments and/or value). Ensure that contracts that appear on proprietary websites (e.g., terms of website use and terms of sale) satisfy the foregoing requirements.

#### **Utilize Appropriate Protective Provisions in Online Terms of Use**

Prominently post on a proprietary website or social media page properly customized notices to help mitigate legal risks. For example, prohibit users from posting content defined as inappropriate, disclaim responsibility for user-generated content or third-party advertisements, limit the company's liability for harm to users resulting from website or webpage use, and reserve the rights necessary to maintain website or webpage security.

#### **Seek Available Immunity for Copyright Infringement**

Given the ease with which material can be obtained and posted online, avoiding copyright infringement based on the use, display, reproduction, or distribution of content posted on social media pages or proprietary websites will always be a concern for e-commerce businesses. The federal Digital Millennium Copyright Act of 1998 (DMCA) lays out certain safe harbors for Internet service providers that could provide protection from such claims. Become familiar with the safe harbor requirements and consider taking the steps necessary to obtain available immunity from claims of copyright infringement.

#### **Avoid Trademark Infringement**

Unlike under the DMCA, there are no statutory safe harbors for trademark infringement claims. Care

must be taken to avoid misuse of third-party marks by seeking consent to use marks and demonstrating a good faith effort to prevent unauthorized use by implementing and following a takedown policy.

#### **Seek Available Defamation Protection**

The federal Communications Decency Act of 1996 offers providers of interactive computer services safe harbor protection from civil liability for defamation (and certain other) claims where the provider is not the content provider. As with the DMCA, implement a policy for acceptable content and utilize a takedown procedure for harmful or offensive material posted by third-party users.

#### **Remember the Rights of Privacy and Publicity**

Privacy laws, including laws designed to protect medical records, financial information, and information about children or teenagers, apply to information collected online. To avoid punitive action from state attorneys general and/or the Federal Trade Commission, prominently post on the website a carefully drafted privacy policy that accurately explains collection practices for personally identifiable information in accordance with applicable laws at the state and federal levels, and strictly comply with any such policy. Similarly, the exclusive right to exploit one's likeness for commercial gain applies to content available online. Procedures should be implemented to control the unauthorized use or disclosure of such protected data and images without permission.

#### **Remember the Impact of Agency Liability**

Remember that actions taken by individuals online (even without the approval of management) can implicate an entity. In particular, actions of employees can expose the company to liability under certain circumstances. Adopt guidelines governing employees' permissible use of company websites, social media pages, and computer equipment and the content that can be displayed or published.

#### **Provide Information Security**

Implement an information security program consistent with the standard generally recognized under federal law and any applicable industry-specific or unique state law requirements in order to protect sensitive data accessible or stored in connection with online websites. Ensure data handling procedures align with any practices described in a website privacy policy.

#### **Be Mindful of Jurisdiction**

Because electronic transmissions through the internet reach parties throughout the world, businesses may become subject to the laws of many different countries or states within the United States when engaging in e-commerce activities. Consider refining the scope of jurisdiction to the extent possible by stating the governing law, venue, or forum and limiting online activities to only those jurisdictions in which the e-commerce business is prepared to comply with applicable laws and regulations.

#### **Know Taxation Obligations**

Whether online transactions and sales are subject to state taxes varies among the states. While certain states have enacted laws that impose obligations on resident businesses or businesses with in-state physical facilities to pay such taxes, others do not currently have a similar requirement. Be aware of those states in which taxes must be collected for online sales and transactions, and keep in mind that any such obligation may change at any time.

#### **Consider Insurance**

E-commerce businesses should consider obtaining insurance coverage in order to limit their financial exposure for information security breaches, online tort and intellectual property right infringement claims, and certain website-specific practices such as hyperlinking, framing, using metatags, and banner advertising.

Please contact one of the authors if you have any questions about this alert.

## ARTICLES

February 3, 2014

### **BRING-YOUR-OWN-DEVICE PROGRAMS: STEPS TO MINIMIZE NONPROFITS' LEGAL RISKS**

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 address 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

## AUTHORS

Armand J. (A.J.) Zottola

## RELATED PRACTICES

Technology Transactions  
and Outsourcing

Labor and Employment

## RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

## ARCHIVES

2015 2011 2007

2014 2010 2006

2013 2009 2005

2012 2008

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](mailto:ajzottola@Venable.com).*

*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.*

## AUTHORS

Armand J. (A.J.) Zottola  
Jeffrey S. Tenenbaum

## RELATED PRACTICES

Advertising and Marketing  
Technology Transactions  
and Outsourcing

## RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

## ARCHIVES

2015 2011 2007  
2014 2010 2006  
2013 2009 2005  
2012 2008

## ARTICLES

November 5, 2013

### GUIDELINES FOR NONPROFITS WHEN NEGOTIATING ONLINE ADVERTISING ARRANGEMENTS

Nonprofits have long looked to advertising and marketing agencies to assist with their marketing and promotion efforts relating to fundraising, membership development, program promotion, product and service sales, and furthering the nonprofit's general purpose and mission. This outsourcing model continues to help nonprofits reach new and existing donors, supporters, members, and other interested third parties, and has not changed with the emergence of online, social media, or mobile advertising. Agencies are not only assisting with development of digital creative materials, but also with advertisement placement, serving, and delivery. With respect to these online initiatives, nonprofits should acknowledge and address the legal risks and issues associated with these new online or mobile delivery arrangements.

The best defense available to nonprofits against these potential pitfalls has been and remains their written agreements with the agencies. Do not rely on a general or outdated contract form. Below is a list of suggested concepts that should be addressed and incorporated, as applicable, into nonprofits' agreements with advertising and marketing agencies. Consideration should also be given to the constantly evolving legal framework governing the following:

- **Retaining Content Ownership.** Specify that the nonprofit owns and retains all intellectual property and proprietary rights associated with its content and data, which is compiled, modified, derived, developed, created, or otherwise used by the agency on the nonprofit's behalf during the term of the agreement. Nonprofits should require, at a minimum, that agencies receive only a tailored license grant to use such content or associated rights, and generally no rights upon termination of the agreement.
- **Confidentiality.** Establish that the nonprofit's confidential information, including, without limitation, any new program offerings, marketing or sales plans, or pricing initiatives, shall be retained by the nonprofit and may be accessed and used by the agency only as necessary for the sole purpose of fulfilling the obligations set out in the agreement.
- **Third-Party Intellectual Property.** Require the agency to obtain the nonprofit's prior written consent or, at a minimum, undertake and perform any necessary rights clearance, before using in any advertising campaign any intellectual property or data owned or held by a third party.
- **Search Engine Optimization.** Legal uncertainty surrounds certain search engine optimization practices and may be outright prohibited, particularly in connection with metatag usage or keyword triggering. Consequently, a nonprofit should require an agency to abide by applicable laws and otherwise remain solely liable and responsible with respect to the utilization of such techniques.
- **Data Collection.** The agency should be bound by both applicable laws and industry guidelines, as well as any other parameters suggested by the nonprofit, with respect to the permissible data, especially personally identifiable or location-based data, that can be collected from advertisements.
- **Data Usage.** Any further use of data collected in an authorized fashion by the agency, especially for purposes unrelated to the original campaign, should be resolved and determined by both the agency and the nonprofit.
- **Distribution.** Absent prior written consent or subject to express parameters, restrict the agency's ability to place advertisements, particularly in contextual-based environments or environments that do not contain general audience content.
- **Deception and Substantiation.** Prohibit the agency from making any additional statements about a nonprofit's products or services without prior and express consent.
- **Comparative Advertising or Endorsements.** To the extent comparative advertising or

endorsements will be implemented as a part of a campaign, maintain control over and otherwise allow for validation of any declarations in order to avoid and otherwise preclude deceptive, confusing, or disparaging practices.

- **Industry-Specific Rules.** Require the agency to comply with any specialized industry rules generally applicable to the planned advertising tactics or the particular industry in which the nonprofit operates.
- **Advertising Guidelines and Best Practices.** Agreements should incorporate, as applicable and as warranted, the best practices advocated by industry standards bodies, such as the Internet Advertising Bureau and the Association of National Advertisers, which provide governing or performance rules for advertising arrangements.
- **Email Marketing.** To the extent the campaign incorporates email communication, require any related email advertisements to include the required notices and mechanisms to comply with applicable laws.
- **Antitrust.** Members of trade and professional associations always must be careful to avoid sharing information, engaging in discussions, or undertaking other practices that could lead to violations of federal and state antitrust laws. Require the agency to represent that it will not make any agreements or otherwise undertake any actions on the nonprofit's behalf which are actually or potentially anticompetitive.
- **Intent-Based Advertising.** Require any agency that utilizes intent-based techniques or technologies to comply with any disclosure, consent, or data-handling or collection obligations both as prescribed by law as well as by generally recognized industry guidelines or self-regulatory rules.
- **Children.** Be especially cautious of allowing an agency to facilitate and market to children under the age of 13 and always require compliance with both applicable laws and generally recognized industry guidelines or self-regulatory rules.
- **Network Connections.** Require the agency to ensure that any access to a nonprofit's systems or networks utilizes software or other processes to prevent unauthorized access or harmful programming code.
- **Termination.** Require the agency to return or destroy all proprietary content upon termination of the agreement, and to cease stating or implying any affiliation with the nonprofit post-termination.
- **Agency Relationship.** Require the agency to acknowledge its role as an independent contractor permitted to act only in accordance with particular parameters and the nonprofit's directives. Require the agency to accept and assume sole responsibility for all other actions or undertakings.
- **Indemnification.** Require indemnification of the nonprofit by the agency for third-party claims.
- **Subcontractors.** Require that agency contracts with media companies or other subcontractors contain, as applicable, and as tailored to the subcontractor's activities, provisions that incorporate or account for the concepts mentioned above.

---

For more information, please contact Armand J. (A.J.) Zottola at [ajzottola@Venable.com](mailto:ajzottola@Venable.com), or Jeffrey S. Tenenbaum at [jstenenbaum@Venable.com](mailto:jstenenbaum@Venable.com).

## ARTICLES

September 2013

### ALLOWING USER-GENERATED CONTENT ON SOCIAL MEDIA: STEPS FOR MINIMIZING NONPROFITS' LEGAL RISKS

#### AUTHORS

Armand J. (A.J.) Zottola

#### RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

Digital Media

#### ARCHIVES

2015 2011 2007

2014 2010 2006

2013 2009 2005

2012 2008

Allowing donors, supporters, members, or other interested third parties to communicate with and about a nonprofit through its social media networks can facilitate and improve a nonprofit's communication and marketing efforts, aid in fundraising and membership development, and otherwise help further the nonprofit's mission. Nonprofits may therefore allow and even encourage third parties to post messages or display content to the nonprofit's controlled social media pages. However, allowance of user-generated content on social media pages controlled or operated by a nonprofit can raise a number of potential legal risks and liability issues, which are due in large part to the fact that the nonprofit may not have complete control over what a third party posts or displays. Below is a non-exhaustive list of legal steps to consider that will help minimize the likelihood that legal liability arises from user-generated content posted to a nonprofit's social media pages.

**Know the Role:** Establish and know when a communication or posting is published or edited on behalf of the nonprofit, and when a posting or other content is provided by a third party (and thus, outside of the nonprofit's control).

**Monitoring:** Although controls should be established to ensure an editorial role only when desired, it is still important to monitor all social media pages controlled or operated by the nonprofit for problematic postings in order to be in a position to take timely and responsive action.

**Terms of Use:** Establish clear policies regarding appropriate content, disclaiming responsibility for user-generated content, providing for removal of posts containing prohibited content, and precluding posts containing prohibited content.

**Take-Down Action:** Prohibit and remove posts containing content that is abusive, offensive, intimidating, humiliating, obscene, profane, discriminatory, irrelevant to the nonprofit's work, or otherwise inappropriate.

**Advertising:** Be mindful of posts containing product and service advertisements because of federal and state rules and guidelines governing advertising and potentially requiring additional compliance obligations.

**Immunity for Copyright Infringement:** Given the ease with which material can be obtained and posted online, avoiding copyright infringement claims based on the use, display, reproduction, or distribution of content posted on social media pages will always be an important concern for nonprofits. The federal Digital Millennium Copyright Act of 1998 (the "DMCA") lays out certain safe harbors for Internet service providers that could provide protection for nonprofits from such claims in this area. Every nonprofit should become familiar with the safe harbor requirements and consider taking the steps necessary to obtain statutory immunity.

**Trademark Infringement:** Unlike under the DMCA, there are no statutory safe harbors for trademark infringement claims. The safest approach is for nonprofits to prohibit posts containing third-party trademarks absent consent from the trademark owner, and to demonstrate a good-faith effort to prevent and manage trademark infringement by implementing the same take-down policies required to obtain immunity under the DMCA.

**Content Attribution:** Ensure that the nonprofit can verify and distinguish its own posted material from messages or materials posted by users. Consider requiring use of a <sup>TM</sup>, ®, and/or © symbol in connection with prominent placements of the nonprofit's intellectual property on social media pages, and otherwise provide notices and conditions for any use or display of the nonprofit's intellectual property by third parties.

**Rights of Privacy and Publicity:** Nonprofits should remember that privacy laws, including laws

designed to protect medical records, financial information, and the privacy of children under the age of 13, still apply to posts made on social media sites. Moreover, the exclusive right to exploit one's likeness for commercial gain similarly applies to social media environments. Restrictions should be stated to control the use or disclosure of such protected data and images without permission.

**Defamation:** Editing, displaying, or distributing posts containing defamatory statements about a third party could lead to civil liability. The federal **Communications Decency Act of 1996** offers providers of interactive computer services safe harbor protection from civil liability for defamation (and certain other) claims where the provider is not the content provider. As with the DMCA, nonprofits should be well versed in the safe harbor requirements and pattern their behavior to qualify for this protection when possible.

**Guard against Antitrust Risks:** Social networking sites and related media can make it easy for members of trade and professional associations to let their guard down and share information or engage in discussions that could lead to violations of federal and state antitrust laws. Remind members that they may not communicate via nonprofit-sponsored social networking to make anticompetitive agreements such as agreeing to restrict production or services, to share competitively sensitive information such as (but not limited to) pricing information, to engage in group boycotts, or to engage in other anticompetitive conduct.

**Employer-Employee Issues:** Remember that content generated by employees (even without the approval of management) can expose the nonprofit employer to liability. Consistent with the recommendation for knowing a nonprofit's role, consider adopting a policy or guidelines for employees governing their use – both "on" and "off-the-clock" – of social media sites; this has now become the norm with nonprofits.

**Retain Records:** Nonprofits using social media should retain records related to such use for a reasonable period of time in the event the records are needed in connection with a federal or state agency investigation, lawsuit or arbitration, or other legal proceeding.

**Posts Are More Public than You Think:** As always, be careful about which posts are permitted to remain on social media pages and always assume that greater (not less) publication or disclosure is possible.

Nonprofits should consider carefully the above issues and guidance and then develop a social media strategy that is properly tailored to their planned goals, activities and concerns.

\* \* \* \* \*

For more information, contact **A.J. Zottola** at [ajzottola@Venable.com](mailto:ajzottola@Venable.com).

*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.*



## AUTHORS:

Armand Zottola  
[AJZottola@Venable.com](mailto:AJZottola@Venable.com)  
202.344.8546

Robert Parr  
[RFParr@Venable.com](mailto:RFParr@Venable.com)  
202.344.4594

MAY 2013

## Guidelines for Protecting Company Trade Secrets

“Trade secrets” are generally defined as confidential proprietary information that provides a business with a competitive advantage or actual or potential economic benefit. Trade secrets are protected under the Economic Espionage Act of 1994 (EEA) at the federal level, and 48 states have enacted statutes largely patterned upon the Uniform Trade Secrets Act<sup>1</sup> (UTSA) (collectively, “Statutes”). Under these Statutes, company information that may be protectable as a trade secret must specifically have three characteristics:

- i. the information must fall within the defined “information” eligible for protection;
- ii. such information must derive independent economic value from not being generally known or readily ascertainable by appropriate means by others; and
- iii. the information must be the subject of reasonable efforts to maintain its secrecy.

Trade secret theft and economic espionage against U.S. companies continue to accelerate. Even a single trade secret security breach may substantially undermine a company’s ability to compete in the marketplace. In recognition of this threat, Congress and certain state legislatures have recently passed some legislation that has broadened and strengthened trade secret protection. Consequently, it has become important for private sector businesses to ensure that they sufficiently safeguard all proprietary and customer information that may qualify as protectable trade secrets. To that end, this guide provides jurisdiction-neutral explanations of key trade secrets concepts, and offers pointers on how to identify and sufficiently protect potential trade secret information.

### (1) Determine Which Data Constitutes “Information”

There is no bright-line definition as to what subject matter constitutes “information” under the Statutes. The aforementioned statutes generally define “information” broadly to include:

- All forms and types of financial, business, scientific, technical, economic, and engineering information;
- Patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, or codes;
- Information related to single or multiple events, negative data points that have commercial value such as the results of lengthy and expensive research which prove that a certain process will not work; and
- Information that can be held or stored in any medium (whether physically, photographically, graphically, electronically, or in writing).

---

<sup>1</sup> Some jurisdictions, such as Texas, California, Arkansas and Illinois, have adopted trade secret laws that depart substantially from the UTSA. Therefore, businesses should carefully research local trade secret laws in the relevant jurisdiction(s) in addition to following this guidance to ensure that they adequately identify and protect all potential trade secret information.

Courts have similarly interpreted “information” to cover virtually any knowledge, data or process used to conduct business that is protected from public disclosure. For example, the following categories of information have been found by courts of law to constitute trade secrets:

- Pricing techniques
- Marketing techniques
- The identity and requirements of customers
- Financial information
- Customer information
- Maintenance of data on customer lists and needs
- Sources of supplies
- Pricing data and figures
- Manufacturing processes
- Product compositions
- Expiration lists (often used in the insurance industry)
- Buy books
- Cost books
- Customer books or lists
- Confidential costs

As a result, businesses should realize that vast amounts of their data may constitute “information” eligible for trade secret protection.

## 2) “Economically Valuable” and “Not Readily Ascertainable” Information

Information must also retain “economic value” and not be “readily ascertainable” by others. Although determined subjectively at first by the claimant, courts of law determine whether information satisfies this standard on a case-by-case basis depending on the unique facts and circumstances of a proceeding. However, when determining value and whether information is readily ascertainable, courts of law generally consider the following factors:

- Reasonable protective measures (not all conceivable efforts) have been established to protect the information from both internal and external theft or misappropriation;
- The information is known by a limited number of employees or other parties (in a “confidential relationship” with the company) who possess a business-need-to-know;
- The information has actual or potential commercial value to a company or provides a company with a competitive advantage in the marketplace;
- The company devoted significant time, money and other resources to develop the information;
- The information would be useful to competitors and requires a significant investment of time, expense or effort to duplicate or acquire, even if some or all competitors possess the know-how and means to independently create their own versions of the information; and
- The information is not generally known to the public, or to other persons or businesses outside of the company who can obtain economic value from its disclosure.

The more of these factors that apply to particular company information, the greater the likelihood a court of law would ultimately conclude the information constitutes a trade secret.

## 3) Implement Reasonable Protective Measures to Ensure Secrecy

Information that retains economic value and is not readily ascertainable must also be subject to reasonable security measures. Businesses should implement reasonable technical, administrative, contractual and physical safeguards appropriately tailored to the day-to-day business of the particular enterprise, the confidential information sought to be protected, the community in which the company operates, and the established awareness of the individual participants to whom access to the information may be granted. Appropriate security measures should result from some consideration of the foregoing factors and an assessment of what safeguards are most compatible with the practicalities and efficiencies of the unique workplace.

### A. WRITTEN INFORMATION SECURITY POLICIES

Companies should implement written information security and confidentiality programs that incorporate proven information security and confidentiality principles. These programs should be regularly and consistently enforced in order to satisfy the third element of the trade secrets test. Below is a list of some suggested measures that companies may adopt to protect confidential information that is eligible for trade secret status:

- *Risk identification and assessment.* Use commercially reasonable efforts to (i) identify and assess reasonably foreseeable threats to the security of confidential information; (ii) identify and assess the likelihood of harm and

potential damage flowing from such threats; and (iii) gauge the need to adjust security protocols to address new threats and program deficiencies.

- *Safeguards.* Implement certain administrative, technical and physical safeguards to prevent the unauthorized access to and use or disclosure of confidential information:
  - **Administrative Safeguards**
    - *Compartmentalize information.* Restrict access to confidential information on a business-need-to-know basis. These restrictions could include dividing information into pieces and precluding all but a few employees from having access to the entirety.
    - *Use unique employee identifiers.* Assign each employee with computer access a unique identification number to enable system tracking.
    - *Audit security protocols.* Regularly review the efficacy of security procedures to address new threats and program deficiencies.
    - *Legending materials.* Classify information according to type and sensitivity and mark documents with an appropriate legend (such as “confidential” or “top secret”).
    - *Distribute employee manuals.* Circulate an employee handbook that (i) outlines what constitutes confidential information or a “trade secret”; (ii) explains the essential nature of the information security and confidentiality program; (iii) reproduces the material terms of any restrictive covenants; and (iv) describes company policies regarding social media use, remote access and mobile devices, and employee privacy.
    - *Conduct employee training.* Regularly train employees about information secrecy, and issue periodic reminders about secrecy obligations.
    - *Entrance interviews.* Conduct entrance interviews for new hires to determine whether they are subject to restrictive covenants with former employers or whether their new employment status raises a substantial likelihood that the company will improperly use a former employer’s trade secrets.
    - *Exit interviews.* Conduct exit interviews with departing personnel to (i) review secrecy obligations and restrictive covenants; and (ii) require the departing employee to sign a statement providing that such employee has returned all company materials containing confidential information, and understands and agrees to abide by post-employment obligations.
    - *Review released content.* Review company advertising, websites, press releases, seminar content and articles before publication to ensure that trade secret information is not inadvertently disclosed.
    - *Consideration of response plan.* Consider implementing a trade secret breach plan that calls for (i) injunctive relief when the perpetrator is known and the trade secret has not yet been widely disseminated; or (ii) a general exclusion order from the U.S. International Trade Commission to bar the importation of goods resulting from unfair trade practices; or, in the extreme case and as a last resort, (iii) an application for patent protection.
  - **Technical Safeguards**
    - *Encrypt data.* Encrypt confidential information that is stored and transmitted across open, public networks.
    - *Technical restrictions.* Limit access to confidential information through passwords and network firewalls.
    - *Run antivirus software.* Use and regularly update antivirus software on all systems commonly affected by malware.
    - *Avoid default passwords.* Do not use vendor-supplied defaults for system passwords and other security parameters.
    - *Catalogue data access.* Track and monitor all access to network resources and confidential information.
    - *Monitor large downloads and emails.* Monitor sizeable downloads or emails with large attachments to help quickly detect potential theft of confidential information.
  - **Physical Safeguards**
    - *Guards.* Station security personnel at each facility entrance.

- *Signage.* Post warning or cautionary signs in areas near where confidential information is located.
- *Limit visitor access.* Provide limited visitor tours of company plants and facilities, if at all.
- *Surveillance.* Establish security and surveillance procedures to prevent any unpermitted entry into company facilities or removal of confidential information.
- *Physical barriers.* Lock up hardcopy materials and require key-card access to sensitive areas of company facilities.

## B. CONTRACTUAL METHODS

Business relationships with parties that may involve disclosure or exposure to company information pose significant threats to the confidentiality of such information. Below is a list of suggested concepts that should be incorporated, as applicable, into businesses agreements with employees, licensees, service providers, contractors, subcontractors, consultants and prospective purchasers of all or part of a business (together, "Business Counterparties").

- *Confidentiality.* Establish permitted uses and disclosures of confidential information by Business Counterparties, and provide that such parties cannot use or further disclose confidential information except upon the written consent by the company or as permitted or required by the contract or law.
  - *Disclosure and assignment of inventions.* Consider coupling nondisclosure requirements with assignment of invention or work obligations. In particular, require employees to promptly and fully inform the company in writing of any inventions, discoveries, works, concepts and ideas ("Developments") created by the employee.
  - *Contractors.* Ensure that contractors are similarly required to inform the company of any Developments created during performance of their duties.
- *Terms of employment.* Require employees to execute written agreements that establish, among other things, clear policies regarding (i) the right to download confidential information onto external or mobile devices; (ii) the ownership and control of confidential information, including, without limitation, work-related social media accounts and confidential information saved on external or mobile devices; (iii) the return or destruction of information upon resignation; and (iv) the obligation to provide notice about subsequent places of employment and the employee's proposed activities or duties for the new employer.
- *Disclosure of restrictive covenants.* Require new employees to represent in writing that they are not currently bound by a covenant not to compete or a nonsolicitation clause with a prior employer.
- *Possession of another's confidential information.* Require new employees to represent in writing that they will not utilize or disclose any confidential information belonging to a prior employer during their tenure at the new company. Companies should also provide employees with the opportunity to decline assignment of rights to intellectual property created or developed under a prior employment relationship.
- *Return of confidential materials.* Require employees of the company and, in particular, new employees, to promise that upon termination, they will promptly deliver to the company all confidential materials.
- *Restrictive covenants.* Consider having employees sign nonsolicitation and/or noncompetition agreements that restrict a narrowly specified scope of activity for a reasonable period of time and within a reasonable geographic territory. The legal rules governing the enforceability of these clauses varies widely among the states. Therefore, carefully research statutes and case law on the enforceability of restrictive covenants in the relevant jurisdictions before implementation.
- *Third-party contracts.* Require contracts with Business Counterparties to contain, as applicable, and as tailored to the Business Counterparty, provisions that include the abovementioned concepts. Additionally, require Business Counterparties to ensure that any subcontractor they engage on their behalf agrees to the same restrictions and conditions that apply to the Business Counterparty with respect to confidential information.

If you have any questions about this alert, please contact one of the authors or a member of the [Technology Transactions & Outsourcing Practice Group](#)

## ARTICLES

September 8, 2011

### NEW GUIDANCE FOR NONPROFITS REGARDING SOCIAL MEDIA POLICIES AND PUNISHMENT

In our last alert on this subject,<sup>1</sup> nonprofit employers were reminded that rapidly developing law in the area of disciplining employees for voicing workplace gripes in social media such as Facebook or Twitter warranted caution before punishment of such behavior, as well as a review of policies that might be found to unlawfully impinge on employee rights under the National Labor Relations Act ("NLRA"). Two recent developments – the issuance of guidance by the Acting General Counsel of the National Labor Relations Board ("NLRB") and the issuance of the first decision by an administrative law judge finding a violation of the NLRA for Facebook-related firings – provide important additional instruction.

As we indicated in our last alert on this topic, because nonprofits are typically not unionized, they have often overlooked the NLRA as a possible limitation on their right to discipline or terminate employees at will. But nonprofits do so at their peril, as these new developments make clear that nonprofits seeking to enforce work rules or restrain employee criticism of them or their policies in social media must take into account the provisions of the NLRA, regardless of whether the nonprofit is unionized.

Cognizant of the growing scope of the issues regarding the legitimate and protected use of social and other media, the NLRB's Acting General Counsel on August 18, 2011 released a report discussing cases involving social media. The report provides very helpful guidance for nonprofits on what policies and punishment for postings may be problematic. For example, the NLRB report discusses the following findings in particular cases:

- Employees were unlawfully discharged for responding to the Facebook posting of a co-worker discussing working conditions, even though the employee who initiated the cyber conversation considered her co-workers' comments to be cyber-bullying and harassment.
- A policy that prohibited employees from posting pictures of themselves depicting their company in any way, including uniforms, corporate logos, or vehicles, was overbroad because it could be interpreted to prohibit employees from posting pictures of themselves engaged in concerted protected activity, such as picketing or other protests against their employer.
- A bartender who complained on Facebook to his stepsister, a non employee, that he had not had a raise in five years, said he was doing "waitress" work without tips, and called the customers rednecks and stated that he hoped they "choked on glass as they drove home drunk" was lawfully fired because the employee did not discuss the posting with his co-workers and there was no evidence that any co-workers responded to it.
- An employee was lawfully discharged after posting profane comments on Facebook critical of store management because the employee's postings were merely an expression of individual gripes as opposed to protected concerted activity. In this case, at least two co-workers responded to the posting; however, their messages reflected that the posting was individual and not group activity.
- A policy prohibiting employees from making disparaging comments when discussing the company or its supervisors was unlawful because the policy did not make clear that it did not prohibit protected concerted activity.
- The discharge of a recovery specialist in a residential facility for homeless individuals who posted demeaning comments concerning her employer's clientele was lawful because there was no evidence of protected concerted activity: the comments did not mention any terms or conditions of employment, the posting was not discussed with any co-workers, and the comments were not for the purpose of inducing group activity or an outgrowth of collective concerns of the employee or her co-workers.

In the wake of the NLRB's guidance document, on September 2, 2011, a NLRB administrative law judge

## AUTHORS

Ronald W. Taylor  
Jeffrey S. Tenenbaum

## RELATED PRACTICES

Labor and Employment

## RELATED INDUSTRIES

Nonprofit Organizations  
and Associations

## ARCHIVES

2015 2011 2007  
2014 2010 2006  
2013 2009 2005  
2012 2008

issued the first adjudicated decision involving social media-based discipline. In the case, *Hispanics United of Buffalo, Inc.*, a nonprofit that renders social services to economically disadvantaged clients in Buffalo, New York was found to have committed unfair labor practices when it discharged several employees for Facebook postings – made on their own computers outside of working hours – that expressed criticism of their working conditions and of a domestic violence advocate who worked for the nonprofit. The advocate complained about the postings to the nonprofit's executive director, who terminated the employees based on the contention that the postings constituted cyber-bullying and harassment in violation of the nonprofit's policies. The ALJ found the comments protected and rejected the contention that the employees were bullying the advocate or that they harassed her in violation of the nonprofit's policies. Consequently, the ALJ concluded that the employees had not engaged in conduct that converted their concerted activity from protected to unprotected status.

The NLRB's recent report and the *Hispanics United of Buffalo* decision provide helpful guidance to nonprofits not wishing to become potential NLRB cases, including the following:

- Communications that are not concerted are generally not protected. However, the cases highlight that a finding of concerted activity may turn on evidence not readily available to the employer, so caution is warranted.
- Communications that are concerted (*i.e.*, that are not merely an individual gripe) on matters of mutual concern to employees are likely to be found to be protected by the NLRA.
- Communications that are protected do not become unprotected simply because the comments are communicated via the Internet and/or because they may be read by nonemployees as well.
- Communications that are protected do not become unprotected just because they contain some critical (about the employer) or otherwise objectionable language.
- A work rule that, reasonably interpreted, would tend to "chill" employees in the exercise of their rights under the NLRA is likely to be found unlawful by the NLRB if challenged. Such a "chilling" effect may be found to exist if a rule explicitly restricts protected activities or, if not, if employees would reasonably construe the rule to prohibit protected activity, the rule was promulgated in response to union activity, or the rule has been actually applied to restrict protected activity.

The spate of cases before the NLRB, including *Hispanics United of Buffalo*, and its recent report on social media cases, reiterate the need for nonprofits to: (1) review their relevant employment policies to ensure that they are not overbroad and do not constitute potential unfair labor practices in and of themselves; and (2) proceed cautiously when determining whether to discipline an employee because of his or her comments in postings on Facebook, Twitter or other social media in order to avoid potential unfair labor practice claims.

---

<sup>1</sup> **[Nonprofits Beware: Your Employees' Blogs, Facebook Posts, and Twitter Tweets May Be Protected by the National Labor Relations Act](#)**