VENABLE® LLP

Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting

September 18, 2013

Venable LLP

Washington, DC

Moderator:

Jeffrey S. Tenenbaum, Esq., Venable LLP

Panelists:

A.J. Zottola, Esq., Venable LLP

Krista S. Coons, Esq., Venable LLP

Presentation

VENABLE® LLP

Keeping Up with Technology and the Law: What Your Nonprofit Should Know about Apps, the Cloud, Information Security, and Electronic Contracting

Wednesday, September 18, 2013, 12:30 p.m. – 2:00 p.m. ET
Venable LLP, Washington, DC

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

Panelists:
A.J. Zottola, Esq., Venable LLP
Krista S. Coons, Esq., Venable LLP

© 2013 Venable LLP

VENABLE® LLP

Upcoming Venable Nonprofit Legal Events

October 24, 2013 – The IRS Final Report on Nonprofit Colleges and Universities: Lessons for All Tax-Exempt Organizations

December 5, 2013 – Work & Family: What Nonprofit Employers Should Know about Family-Oriented Employment Laws

© 2013 Venable LLP

VENABLE LLP

Agenda

- Apps
- The Cloud
- Information Security
- Electronic Contracting

© 2013 Venable LLP

VENABLE® LLP

So You Want to Create an App? Legal Considerations for Nonprofits

© 2013 Venable LLP

But, What Exactly Is an App?

- A software application designed to run on smartphones, tablet computers, and other mobile devices
- A user can download the app to a personal device (e.g., smartphone, tablet) from any number of application distribution platforms, which are usually operated by the owner of the operating system on that mobile device, e.g., Apple App Store, Google Play, Windows Phone Store, and BlackBerry App World

© 2013 Venable LLP

Legal Considerations: IP for Apps

- Copyright
  - Protects the tangible expression of the app itself, including its code, all words and images, and the audiovisual display (i.e., look and feel)
- Trademark
  - Protects all use of your company name, any logos, brands, product names, trade dress
- Patent
  - Protects inventive concepts

© 2013 Venable LLP

Why Does IP Ownership Matter?

- Only an IP owner intrinsically has the right to stop others' unauthorized use of that IP
- Only an IP owner has the right to profit from others' authorized use of that IP
- In some cases, others' unauthorized use of your IP may dilute the strength of your IP, e.g., trademarks
- Even the best intentions can be spoiled!!

© 2013 Venable LLP

Contractors and Work Made for Hire

- General Rule: All independent contractors and volunteers should sign a written work-made-for-hire agreement and copyright assignment
- A "work made for hire" is a work specially ordered or commissioned [if it fits into one of nine enumerated categories and] . . . if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. 17. U.S.C. § 101
- Include a copyright assignment as a fallback
- BUT, can't contract around the law

© 2013 Venable LLP

Protecting Your IP

- Registration
  - Copyright
  - Trademark
  - Patent
- Ensure proper, visible usage of the IP symbols within the app
- Ongoing process

© 2013 Venable LLP

User Licenses and Terms of Use

- Can be click-through
- Provide user with the legal right to install and use
- Contain basic legal and support terms
- Provide restrictions on user's ability to use, share, copy, etc.
- Does the platform require certain terms?
- Provide you the right to use content uploaded by user
- How will you use data – push notifications?
- Pitfall! Beware integration with other digital media – be sure your terms don't conflict.

© 2013 Venable LLP

Money Traps

- Make all fees (if any) clear and unambiguous
- If there will be an in-app purchase option, make that clear and unambiguous
- Fundraising considerations
  - Does your distribution platform permit it?
  - May have to take users to external website
  - What fundraising apps are already out there?

© 2013 Venable LLP

Data Privacy Considerations

- You must have a privacy policy (California AG + Platform "Joint Statement")
- More than lip service, i.e., "privacy by design"
  - What data does the app collect (both intentionally and unintentionally)?
    - Users' mobile device contacts
    - Web browsing activity
    - Location
  - Where is the data stored and for how long?
  - For what purpose is the data collected?
  - Is the data shared or distributed?
- Special concerns regarding children's data

© 2013 Venable LLP

VENABLE LLP

Practical Considerations

- Evaluate whether an app is right for you
- How will you track success?
- Does an app already exist that you can leverage to achieve the same goals?

Questions?

© 2013 Venable LLP

VENABLE® LLP

What is the Cloud?

© 2013 Venable LLP

VENABLE LLP

In General…

A model for enabling:

- Convenient,
- On-demand network access,
- To a shared pool of configurable computing resources,
- That can be rapidly provisioned, and
- Released with minimal effort.

© 2013 Venable LLP

VENABLE LLP

Definitions of Deployment Models

- Private Cloud: Operated solely for an organization. May be managed by the organization or a third party
- Community Cloud: shared by several organizations with shared concerns
- Public Cloud: Made available to general public
- Hybrid Cloud: Composed of two or more clouds (private, community, or public) that remain unique

© 2013 Venable LLP

Data Issues: Overview

- Potentially less privacy
  - More risk of online disclosure
  - Rise of privacy complaints
  - More susceptible to data aggregation and mining
- Information security concerns
- Loss of control and a lot of trust in the provider
- Understand how data will be stored and maintained
- Consider general access privileges, and ease of access, to data
- Consider rights to access and produce data in the event of litigation

© 2013 Venable LLP

Data Issues: Overview (cont'd.)

- How readily and quickly will provider investigate (or facilitate the investigation of) illegal or inappropriate activity?
- Consider rights and access upon termination
  - Right to destroy?
  - Obligation to return
- Understand that there can be new issues with third-party data retention and data destruction
  - Holding too much data or not enough
  - Holding data for too long or not long enough

© 2013 Venable LLP

Data Issues: Overview (cont'd.)

- There may be less control over disaster recovery preparation and response
- More susceptible to general telecommunication or equipment outages
- Balance the cost convenience of the cloud with the potential costs in the event of a data breach
  - Compare against current policies, processes, or capabilities or those offered by competitors

© 2013 Venable LLP

Data Issues: Information Security

- Technical responsibilities, legal consequences
- Remote data storage may not be acceptable under certain contracts
- Available security measures
  - Understand electronic and physical security
  - Required security
  - Reasonable security
  - Consider data breach notification obligations
  - Varying state law responsibilities
  - Data segregation issues
  - Less of an issue with private cloud than public cloud, but more technical headaches

© 2013 Venable LLP

In the Event of Litigation…

- Companies using the cloud may face complications when seeking to preserve and produce data from the cloud
- Factors outside the party's control that could impact that party's access to data
- The data stored in the cloud may be subject to legal and regulatory restrictions of which the company could be unaware
- Data may change physical locations (EU v. US)
- Possession, custody, or control
  - F.R.C.P. 26

© 2013 Venable LLP

In the Event of Litigation: E-Discovery Problems

- Need to account for
  - Litigation hold
  - Preservation obligations
  - Form of production
  - Admissibility of evidence
  - Inadvertent loss of data/sanctions
- Need to know how much data is retained
- Need access to the data and assurances that the data is maintained and retained in the same form
- Is there a payment obligation for release and access?

© 2013 Venable LLP

Compliance Issues

- No regulation on cloud computing…yet
- BUT some federal and state laws MIGHT apply
  - What law governs?
    - Location, location, location
    - Contract may not control
- Certain federal and state law regulations require industry-specific considerations, and potentially, commitments

© 2013 Venable LLP

Conclusion

- Laws and rules will likely change over time
  - Driven by privacy and information security concerns
- Need for clear and consistent communication of policies to meet or set user expectations on data collection and use practices
- Don't store more than you need. Helps to limit liability

© 2013 Venable LLP

VENABLE® LLP

Information Security

© 2013 Venable LLP

VENABLE® LLP

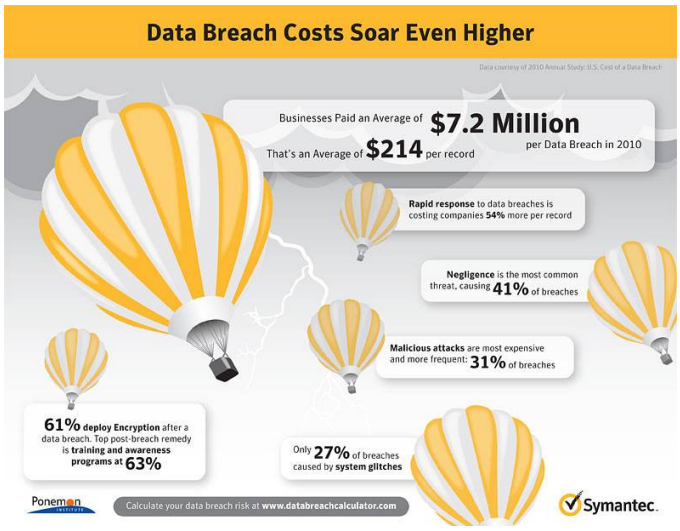
Why Have Security Mechanisms in Place?

- Cost of IT repairs and mitigation activities
- Loss of public image
- Compliance with victim notification requirements
- State/federal investigations
- Defending subsequent civil litigation
  - Average settlement award is $2,500/plaintiff
  - Average attorneys' fees are $1.2 million

© 2013 Venable LLP

VENABLE LLP

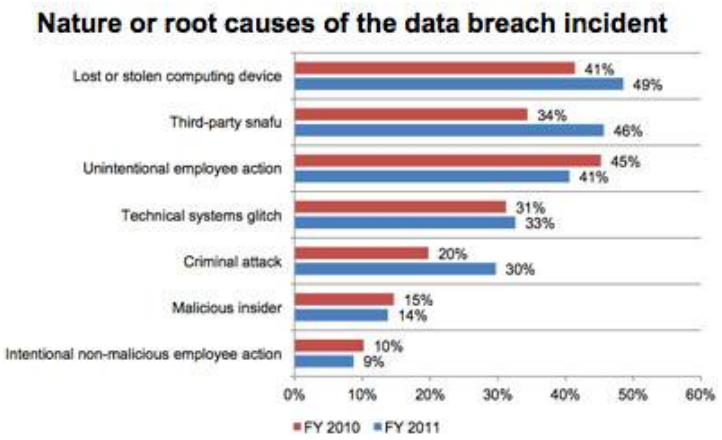
Cost of Data Breach



© 2013 Venable LLP

VENABLE LLP

Employees, not hackers, cause most data loss



© 2013 Venable LLP

Massachusetts Data Security Statute

- Encryption of all transmitted personal information that travels across public networks and wirelessly
- Encryption of all personal information stored on laptops or other portable devices
- Education and training of employees on the proper use of the computer security system and the importance of personal information security
- Detailed written information security policy

© 2013 Venable LLP

State Notification Laws - A General Framework

- Delineating who must comply with the law
- Defining the terms “personal information” and “breach of security”
- Establishing the elements of harm that must occur, if any, for notice to be triggered
- Adopting requirements for notice
- Creating exemptions and safe harbors
- Clarifying preemption and relationships to other federal laws
- Creating penalties, enforcement authorities, and remedies

© 2013 Venable LLP

VENABLE LLP

How to Protect Data

- Cloud computing
- Implement policies regarding BYOD
- Assess the need for certain data
  - Is the personal information necessary to complete a particular task?
- Control access to data
- Educate your employees

© 2013 Venable LLP

VENABLE LLP

Tactical Recommendations

TACTICAL RECOMMENDATIONS (For Malware) Measures	Value	Priority	Effort	Cost
Educate Users	High	High	Low	Low
Use Anti-virus and Anti-malware	High	High	Medium	Medium
Keep Systems Patched and Up-to-date	High	High	Medium	Medium
Remove Administrative Access and Limit User Privileges	High	High	Medium	Medium

TACTICAL RECOMMENDATIONS (For BYOD) Measures	Value	Priority	Effort	Cost
Educate Users	High	High	Low	Low
Keep Systems Patched and Up-to-Date	High	High	Medium	Medium
Enforce a Device Policy	High	High	Medium	Medium
Deploy Mobile Anti-virus and Mobile End-point Protection	Medium	Medium	Medium	Medium

Source: Solutionary 2013 Global Threat Intelligence Report

© 2013 Venable LLP

What To Do When a Breach Occurs?

- Deal with security issues ASAP
- Conduct an investigation
- Report the breach and inform the victims
  - Involve law enforcement as necessary
  - 46 states require that victims of data breach are notified
- Prepare a public statement

© 2013 Venable LLP

Conclusion

- Be familiar with laws governing protection of personal information
- Protect information to avoid a breach
- Educate your employees regarding privacy and security

© 2013 Venable LLP

VENABLE® LLP

Electronic Contracting

© 2013 Venable LLP

VENABLE® LLP

Formation of a Contract

- Offer
- Acceptance
- Consideration

© 2013 Venable LLP

Is a Writing Even Necessary?

- A written agreement is not always necessary
  - Handshake agreement
  - Oral agreements
- Some contracts/signatures however need to be in writing to be enforceable
  - State law
    - Statute of frauds
  - Federal law
    - Copyright/trademarks/patent agreements
    - Consumer notices/disclosures

© 2013 Venable LLP

Federal v. State Law

- State: Uniform Electronic Transactions Act (UETA)
  - Governs transactions involving businesses, commercial entities and government affairs
- Federal: Electronic Signatures in Global and National Commerce (E-SIGN)
  - Governs transactions subject to federal law
  - Governs in the absence of state law

© 2013 Venable LLP

VENABLE LLP

Intent to Conduct Transaction Electronically

- UETA as a set of default rules
  - Parties may opt out
  - If parties agree otherwise, UETA will not apply
- Hypothetical
  - Joe gives out his business card with his business e-mail address on it. What would be reasonable for the recipient of the card to infer from this exchange?
- Intent to conduct transactions electronically, not intent to communicate electronically

© 2013 Venable LLP

VENABLE LLP

Questions?

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

A.J. Zottola, Esq.
AJZottola@Venable.com
t 202.344.8546

Krista S. Coons, Esq.
KSCoons@Venable.com
t 212.503.0552

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

© 2013 Venable LLP

Speaker Biographies

VENABLE® LLP

our people

Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

jstenenbaum@Venable.com

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

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

AREAS OF PRACTICE

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

INDUSTRIES

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

GOVERNMENT EXPERIENCE

Legislative Assistant, United States House of Representatives

BAR ADMISSIONS

District of Columbia

REPRESENTATIVE CLIENTS

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

EDUCATION

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

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

MEMBERSHIPS

American Society of Association Executives

California Society of Association Executives

New York Society of Association Executives

Association of Corporate Counsel
Association of Private Sector Colleges and Universities
Automotive Aftermarket Industry Association
Brookings Institution
Carbon War Room
The College Board
Council of the Great City Schools
Council on Foundations
CropLife America
Cruise Lines International Association
Foundation for the Malcolm Baldrige National Quality Award
Gerontological Society of America
Goodwill Industries International
Homeownership Preservation Foundation
The Humane Society of the United States
Independent Insurance Agents and Brokers of America
Institute of International Education
International Association of Fire Chiefs
Jazz at Lincoln Center
The Joint Commission
LeadingAge
Lincoln Center for the Performing Arts
Lions Club International
Money Management International
National Association of Chain Drug Stores
National Association of Music Merchants
National Athletic Trainers' Association
National Board of Medical Examiners
National Coalition for Cancer Survivorship
National Defense Industrial Association
National Fallen Firefighters Foundation
National Fish and Wildlife Foundation
National Hot Rod Association
National Propane Gas Association
National Quality Forum
National Retail Federation
National Student Clearinghouse
The Nature Conservancy
NeighborWorks America
Peterson Institute for International Economics
Professional Liability Underwriting Society
Project Management Institute
Public Health Accreditation Board
Public Relations Society of America
Recording Industry Association of America
Romance Writers of America
Texas Association of School Boards
Trust for Architectural Easements
United Nations High Commissioner for Refugees
Volunteers of America

HONORS

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

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

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

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

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

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

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

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

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

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

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

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

ACTIVITIES

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

PUBLICATIONS

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

SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer on nonprofit legal topics, having delivered over 500 speaking presentations. He served on the faculty of the ASAE Virtual Law School, and is a regular commentator on nonprofit legal issues for *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 Voice of America Business Radio, Nonprofit Spark Radio, and The Inner Loop Radio.

VENABLE® LLP

our people

Armand J. (A.J.) Zottola

Partner — *Washington, DC Office*

T 202.344.8546 F 202.344.8300 ajzottola@Venable.com

Working at the intersection of commerce and technology, A.J. Zottola focuses his practice on the exploitation of intellectual property, intangible, and technology assets in business and strategic relationships.

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

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

His extensive experience also helps clients resolve and craft settlement arrangements for misappropriation and infringement matters and for disputes involving commercial and licensing agreements. In addition, he regularly counsels clients on intellectual property, e-commerce and privacy issues, and prosecutes and manages U.S. and foreign trademark and copyright portfolios.

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

AREAS OF PRACTICE

Technology Transactions and Outsourcing

Corporate

Privacy and Data Security

Franchise and Distribution

Advertising and Marketing Litigation

INDUSTRIES

New Media, Media and Entertainment

Government Contractors

Life Sciences

Nonprofit Organizations and Associations

Green Businesses

BAR ADMISSIONS

Maryland

District of Columbia

EDUCATION

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

Editorial Assistant, *Catholic University Law Review*

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;

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

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

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

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

VENABLE® LLP

our people

Krista S. Coons

Associate — *New York, NY Office*

T 212.503.0552 F 212.307.5598 kscoons@Venable.com

Krista Sirola Coons is a member of Venable's Technology Transactions and Outsourcing Practice Group. Ms. Coons focuses her practice on the protection and enhancement of intellectual property rights and technology assets. She structures and negotiates various intellectual property and technology agreements, including marketing, distribution, technology licensing, outsourcing, software development and hosting agreements. She also has experience in negotiating entertainment-based transactions, including content distribution/licensing, celebrity endorsement, live performance, music publishing and programming deals. Ms. Coons also assists clients with the development and acquisition of intellectual property and the management of worldwide intellectual property portfolios.

In addition, Ms. Coons's practice includes intellectual property counseling and litigation. She 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).

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

BAR ADMISSIONS

New York

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

Additional Information

VENABLE® LLP

Technology Transactions Alert

April 2013

Information Security Implications for Business Agreements

This alert was also published in Law360 on April 22, 2013.

AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr

RELATED PRACTICES

Technology Transactions and Outsourcing

Corporate

ARCHIVES

2013 2009 2005

2012 2008 2004

2011 2007 2003

2010 2006

On February 12, 2013, President Obama signed an Executive Order ("Order") that outlined a voluntary cybersecurity framework ("Framework") designed to help protect the nation's critical infrastructure, which is generally defined as those systems or assets, whether physical or virtual, which are so vital to the United States that their incapacitation or destruction would harm public health or safety, economic security, or national security. The Department of Homeland Security has already designated the following 16 economic sectors as home to the U.S. critical infrastructure: information technology services, energy, telecommunications, banking and financial services, chemicals, manufacturing, transportation, emergency services, food and agriculture, healthcare and public health, the defense industrial base, government and commercial facilities, nuclear reactors, materials and waste, and water and wastewater systems. The Framework may therefore apply to countless companies of all sizes across a wide variety of critical infrastructure industries.

More generally, the Order has important implications for any private sector business because information security has rapidly become a hot button issue in this age of growing economic espionage, intellectual property and trade secret theft, and sensitivity to customer privacy. An increasing number of companies have recently reported data security breaches. Even a single security incident may lead to regulatory penalties, shareholder or customer class-action lawsuits, loss of customers to competitors, and irreparable damage to a company's brand or reputation. A company's best defense against any of these potential pitfalls is to take the steps necessary to sufficiently protect all proprietary and customer data.

Information Security Through Contract Drafting

Private sector businesses should now ensure that their agreements contain terms that effectively control access to and use and disclosure of their confidential or nonpublic intellectual property assets, such as patents, copyrights, and trade secrets ("Intangible Assets") and, separately, the personally identifiable information they store or otherwise retain ("Customer PII"). In an effort to minimize the likelihood of data breaches and the increasing number of data security obligations, businesses should even strive to consider safeguarding any Customer PII they are not presently obligated to protect under the patchwork of industry-specific privacy and information security laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. What follows is a list of suggested concepts that should be incorporated, as applicable, into business agreements with counterparties who may have access to Intangible Assets or Customer PII (collectively, "Company Information").

- ***Confidentiality.*** Establish permitted uses and disclosures of Company Information by service providers, contractors, subcontractors or other venders, or counterparties to transfer, sale, merger or acquisition transactions (together, "Business Counterparties"), and provide that such parties cannot use or further disclose Company Information except as permitted or required by the contract or law.
- ***Risk identification and assessment.*** Consider requiring Business Counterparties to use commercially reasonable efforts to (i) identify and assess reasonably foreseeable threats to the security of Company Information and the likelihood of harm and potential damage flowing from such threats; (ii) classify data according to type or sensitivity; and (iii) gauge the need to adjust security protocols to address new threats or handling and storage deficiencies.
- ***Safeguards.*** Provide that Business Counterparties must implement technical, administrative, and physical safeguards to prevent unauthorized access to or use or disclosure of Company Information. Examples of such safeguards include (i) compartmentalizing Company Information on a business-need-to-know basis; (ii) encrypting stored and transmitted Company Information; (iii)

limiting access to Company Information through passwords, network firewalls, and locking up hardcopy records; (iv) auditing security protocols on a regular basis; and (v) requiring employee information security training.

- ***Incident response and breach notification.*** Require Business Counterparties to report any unauthorized access, use, or disclosure of Company Information within a specified time frame, and provide that they must follow baseline breach notification procedures, including (i) a prompt investigation into the compromised information by designated individuals or groups; (ii) obligations to report (or assist with reporting) breaches to required regulators and law enforcement authorities within a specified time frame; (iii) mitigation procedures designed to limit the dissemination of stolen Company Information; (iv) and obligations to promptly notify affected individuals under certain circumstances.
- ***Customer Privacy.*** Consider inclusion of provisions in privacy policies and agreements with customers which (i) explain the company's practices regarding the collection, use and disclosure of Customer PII in business transactions; (ii) give customers the right to control certain or all secondary uses of their PII, and to access and contest the accuracy of their PII; (iii) explain or reference the procedures designed to ensure the integrity and accuracy of Customer PII; and (iv) describe how customers may seek information.
- ***Restrictive Covenants.*** Require employees to sign enforceable nondisclosure or noncompete agreements to protect Intangible Assets and, in particular, Customer PII from being misappropriated upon resignation.
- ***Terms of Employment.*** Require employees to execute written agreements that establish clear policies regarding downloading Company Information onto external devices, the ownership and control of Company Information, including, without limitation, work-related social media accounts and Company Information loaded onto external devices, and the return or destruction of data upon resignation.
- ***Downstream obligations – subcontractors.*** Require a Business Counterparty to ensure that any subcontractor it may engage on its behalf that will have access to Company Information agrees to the same restrictions and conditions that apply to the Business Counterparty with respect to such information.
- ***Termination rights.*** Retain a right to terminate any contract with a Business Counterparty that violates a material term of its agreement relating to Company Information.
- ***Data access by Business Counterparties.*** Draft provisions that clearly describe the Business Counterparty's rights to access Company Information during the arrangement and, in particular, in the event of litigation.
- ***Data destruction or return.*** After contract termination, require Business Counterparties to return or destroy all data received from the company, or created by the Business Counterparty on behalf of the company.

If you have any questions, please contact the authors or a member of the **Corporate** or **Technology Transactions and Outsourcing Group**.

QuickCounsel

Guidelines for Creating Enforceable Contracts Online - "The New Way is the Same as the Old Way"

By A.J. Zottola, Partner in the Technology Transactions & Outsourcing Group of Venable LLP, and Robert Parr, Associate in the Corporate Group of Venable LLP

Overview
Make an Offer: Notify Contracting Parties that the Terms are Binding
Acceptance: Require Electronic Signature to Affirmatively Manifest Assent
Consideration: Mutual Binding Promises Required for Enforceability
Additional Enforceability Considerations
Record Retention Requirements
Verify the Identity of the Contracting Parties
Amending an Existing Electronic Agreement
Conclusion
Additional Resources

Overview

While bright line rules regarding online agreements are still being developed, courts generally apply traditional contract principles to online contracts. Every online agreement requires an offer, acceptance, and consideration in order to establish an enforceable contractual relationship. State and federal statutes that address online contracts reflect this approach, such as theUniform Computer Information Transactions Act adopted by Maryland and Virginia. This thinking is also shown in related U.S. Federal laws such as the Electronic Signatures in Global and National Commerce Act. The following QuickCounsel identifies the key issues that in-house counsel should consider when creating online agreements, and provides advice on how to properly address those issues.

Make an Offer: Notify Contracting Parties that the Terms are Binding

Definition of offer. An offer is a manifestation of willingness to enter into a binding legal relationship. The essential terms must be sufficiently communicated to the offeree in order to invite valid acceptance.

Content of notice of offer. Compose the terms with simple and unambiguous language that fully discloses all material rights and obligations,and clearly expresses that a binding legal relationship arises upon the contracting party's acceptance.

Practice tips for making offers:

Write the terms in a font that is easy to read and language that is not susceptible to more than one reasonable

interpretation.

Consider also offering a summary of key terms in a notice, especially for material and closely scrutinized (contentious) terms, such as arbitration and forum selection clauses.

Prominence of notice. Ensure that all terms are visibly, conspicuously and prominently displayed and, when presented through a website, available on or through a link from the website's primary page (and all other pages, if possible).

Practice tips for providing adequate notice of the offer:

Configure (or try to configure) the webpage so that all terms are viewable upon uploading the page without needing to scroll, download information, access or install software, or make payments for purchases.

Allow contracting parties to easily read and navigate the terms. They should not be pressured to rush through the terms by web-page timeouts, and they should have the opportunity to read the terms as often as they would like before acceptance.

Display the terms on the same screen and near the "accept" button. Offer contracting parties the option to decline as prominently and by the same method as the option to agree.

Consider highlighting important terms in a different color or font size.

Ensure the terms remain accessible online after contract formation.

Separate the terms from marketing text, and make sure they do not contradict other statements made elsewhere on the website.

Customizing notice. Consider whether the target consumer base or audience has special characteristics that may undermine the effectiveness of notice, such as an international consumer base or audience likely requiring notice in multiple languages.

Practice tip for when agreements will likely be made with people in foreign jurisdictions:

Evaluate foreign legal requirements for contract formation to ensure compliance. Be cognizant of content restrictions, language requirements, and limitations on advertising and other promotional activities.

Acceptance: Require Electronic Signature to Affirmatively Manifest Assent

Definition of acceptance. Acceptance is a manifestation of assent to the essential terms based on words or conduct. Electronic acceptance can be effective when sent or communicated, not when actually received or acknowledged.

Assent by electronic signatures. Electronic signatures are an "electronic sound, symbol, or process attached to or logically associated with" an electronic document and "executed or adopted by a person with the intent to sign" the electronic document. Electronic signatures have the same legal effect as ink signatures.

Practice tips for inviting valid acceptance:

Acceptable methods of acceptance. Require the contracting parties to accept the terms by a method that affirmatively signals assent:

Click-through processes, such as checking an onscreen box or scrolling the agreement before clicking "I accept".

Typed signature at the end of an electronic document or email.

Automated electronic signature processes that allow for verification by both parties.

The contracting party expressly affirms that manifesting assent to the terms by the required method constitutes an "acceptance" and gives rise to a contractual relationship.

The contracting party expressly acknowledges that using a website or online service after being provided sufficient notice of the terms and failing to reject them constitutes "acceptance".

Attribution. In anonymous situations, such as many online transactions for general audience sites, consider using security procedures designed to ensure the authenticity of electronic signatures in order to attribute the electronic signature to the party against whom the contract is sought to be enforced.

Practice tip for ensuring attribution:

Document related security procedures and regularly review them to ensure effectiveness and compliance.

Consideration: Mutual Binding Promises Required for Enforceability

Definition of consideration. Enforceable contracts must be supported by consideration–a mutual exchange of promises that represent binding legal obligations.

Illusory promises. A promise is "illusory" when at least one party retains an "unlimited right to decide later the nature or extent of his performance". Therefore, an illusory promise lacks consideration and is unenforceable.

Practice tip for avoiding term invalidation:

Avoid unilateral amendment rights. Terms that permit one party to unilaterally modify the agreement create an illusory promise that is unenforceable.

Additional Enforceability Considerations

Unconscionability

Definition of adhesion contracts. Unilaterally imposed terms of use can sometimes be viewed as contracts of adhesion – agreements drafted and imposed by a party with superior bargaining power on a weaker party, usually a consumer, who adheres to the contract with no real choice about its terms or opportunity to engage in meaningful negotiation.

Practice tip for avoiding contracts of adhesion:

A court may be less likely to conclude that an agreement is a contract of adhesion when the offeree must accept the terms by one of the methods described above that clearly and affirmatively signal assent. The more control the offeree appears to have over the acceptance process, the less likely the court will be to view the terms as being forced upon a weaker and disempowered party.

Shock the conscience standard. Contracts of adhesion are unenforceable when their terms "shock the conscience." Courts determine whether terms cross this threshold on a case-by-case basis depending on the unique facts. Generally, excessively harsh or one-sided terms will be invalidated.

Practice tips for avoiding term invalidation:

Keep in mind that class action waivers, arbitration requirements and inconvenient forum selection clauses have been

identified as examples of controversial terms. Arbitration clauses and forum selection clauses are most heavily scrutinized by the courts.

Balance business interests with fairness to the consumer. Consider whether there is a legitimate business justification to use any of the foregoing terms, such as lowering transaction costs. Even if such a justification exists, evaluate whether it would be substantially unfair to include any of the foregoing terms in an agreement with a consumer of average sophistication.

Violations of Public Policy

Illegal provisions. Terms that are illegal, such as usurious finance charges, are unenforceable. Ensure the terms do not violate state or federal laws.

Unfair trade practices. Terms that violate local and federal consumer protection laws are unenforceable. Do not make false representations about the goods or services, and review federal and state consumer protection laws for compliance.

Record Retention Requirements

Maintain electronic records. Retain a copy of all electronic agreements, including evidence of electronic signatures.

Practice tip for memorializing electronic signature requirements:

Document any electronic signature requirements that are not apparent from reading the terms displayed onscreen to contracting parties. For example, explain in writing that contracting parties cannot accept the terms without first clicking an "I agree" button, and keep this document (and the date of acceptance and the identity of the acceptee) on file.

Accessibility and accuracy requirements. Storage of an electronic record will satisfy legal record retention requirements if:

The electronic copies accurately reflect the actual agreement between the parties:

Given that websites are often redesigned, website proprietors must keep records showing what version of their electronic agreements applied to what contracting parties at what time;

The stored records remain freely accessible for later reference; and

Both parties may download, store or print the agreement without interference.

Records can be kept in electronic-only form, if they meet the above requirements. Such records will also satisfy court evidentiary rules or other rules of law that require transaction records to be kept in original form.

Secondary procedures. Back-up the records with other electronic copies and encourage contracting parties to maintain their own records.

Verify the Identity of the Contracting Parties

Anonymity. Among other issues, the sometimes anonymous nature of online contracting complicates efforts to ensure that the contracting party has the legal capacity to consummate a binding legal relationship, and that he or she is not located in a country subject to export sanctions or other legal requirements, such as age. Consider using different approaches to verify counterparty location and identity.

Commercial identity verification service. These services require a contracting party whose identity is to be confirmed to provide specific personal data to an online identity verification firm for contracting purposes. The firm searches public and private databases for information about that person and requires him to answer questions based on matched records. An identity score is then calculated and the identity of the contracting party is either given the "verified" status, or not, based on the score.

Digital certificate. This device is an electronic document that verifies the authenticity of an encrypted digital signature. The certificate can include name, address, organization affiliation and other information.

Other verification methods. Consider requiring contracting parties to provide other information, such as address or birthday, in text boxes displayed on the computer screen.

Security procedures. These services should supplement, not replace, the internal security procedures designed to ensure the authenticity of electronic signatures that were mentioned above.

Amending an Existing Electronic Agreement

Notice of amended terms. Like with the initial terms, provide adequate notice of the revised terms and inform contracting parties that they may terminate the agreement or affirmatively accept the terms by electronic signature.

Timing. Provide contracting parties with a reasonable amount of time to consider their options, such as 30 days.

Renewals. Consider tying the amended agreement to the effective date of a renewal term.

Closely scrutinized amendments. Courts may be more likely to invalidate amended terms that are presented to customers who receive ongoing services, or when the revised terms expand a company's right to disclose personal information about its customers.

Practice tip to avoid amended term invalidation:

> Consider using a click-through process to obtain clear proof of assent to the new terms.

Conclusion

In-house counsel should remember that traditional contract law principles generally govern online contract formation notwithstanding the fact that some state and federal legislation has been passed that specifically addresses online contracts. When drafting online agreements, therefore, keep in mind the above issues and recommendations in order to maximize the likelihood of drafting enforceable online contracts.

Additional Resources

ACC InfoPAKs: CONTRACTS 2.0: MAKING AND ENFORCING CONTRACTS ONLINE

Uniform Law Commission: ADDITIONAL U.S. LAWS APPLICABLE TO ELECTRONIC SIGNATURES AND CONTRACTS: UNIFORM ELECTRONIC TRANSACTIONS ACT SUMMARY

Government of Canada - Justice Laws Website: SELECTED FOREIGN LAW REGARDING ONLINE CONTRACTS – CANADA: PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Ecommerce Blogs: E-COMMERCE ISSUES AND DEVELOPMENTS: TOP BLOGS

Published on December 20, 2012

Have an idea for a quickcounsel or interested in writing one?

Submit your ideas by filling out our online topic proposal form.

The information in this QuickCounsel should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of its authors, its sponsors, and/or the ACC. This QuickCounsel is not intended as a definitive statement on the subject addressed. Rather, it is intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.

Reprinted with permission from the Association of Corporate Counsel
2013 All Rights Reserved

http://www.acc.com/legalresources/quickcounsel/gfceco.cfm

Understanding the Dark Sides of the Cloud: Top Ten Legal Risks for Cloud Computing Users

Dec 11, 2012

By A.J. Zottola, Partner in the Technology Transactions & Outsourcing Group of Venable LLP, and Alexis A. Martirosian, Associate in the Corporate Group of Venable LLP

What is the Cloud?

The Cloud is an internet-based delivery model that can provide immediate access to various computing resources, which include applications, e-mail, communication, content sharing, and electronic transactions. In connection with implementation of the Cloud, data is initially captured by the outsourcing business, transmitted to the Cloud provider, processed by the provider, stored within the provider's computers, and then remotely accessed via a network. The Cloud can support a client's infrastructure with tools such as computing power and data storage. It can also offer a computing platform for database management, security, and workflow management. Finally, software can be provided to clients through remote access and thus eliminate or lower the expense of more traditional "per-seat" or "per-copy" licensing.

Why is there interest in the Cloud?

With the Cloud, clients can avoid investing in computer hardware and software resources required for on-site computing power. Since users often pay for usage, Cloud computing transforms more expensive IT capital expenditures for equipment into lower operating expenses for services. Another advantage to the Cloud is that it generally removes the need for on-site personnel and support services. Cloud users are not responsible for updates and patches, which are done centrally by the service provider. Perhaps the Cloud's most appealing trait is that users can access their data anywhere that has an internet connection. While the Cloud gifts its users with greater flexibility and lower costs for IT needs, users must be aware of the associated legal risks.

1. Insufficiently specific and balanced contracts with Cloud providers could leave users cornered.

Contracting with Cloud providers without careful consideration can put the user in a very risky position. Users are often offered a form contract filled with unfavorable provisions, such as expansive disclaimers, foreign applicable law, and limitations on the liability of the provider's failures of data integrity, confidentiality, or service continuity. Typically, providers will only offer limited warranties of performance, confined to providing the services in accordance with "good industry practice" or "skill" and "care" even though, in such an immature market-place, it is not known what such standards mean. Contracts can also grant providers an expansive right to use customers' data and materials and include unnecessary services. Before signing agreements, users should fully analyze contract options and plan to negotiate based more specifically on their needs and concerns.

2.Lack of new laws to address the Cloud make users more vulnerable.

Governments across the globe are considering data protection solutions that would update the relevant laws across their particular jurisdictions. As of now, however, U.S. law does not thoroughly address this industry. As a result, the contract between the user and the provider will be the basis of any dispute that arises. Left un-negotiated, this contract will almost always benefit the provider. Users can avoid this by negotiating dispute resolution provisions with consequences they can better tolerate.

3. Multiple service locations expose users to unforeseen jurisdictions.

Seemingly easy litigation assessments, such as which jurisdiction controls, can be more complex in Cloud contract disputes. Cloud services can be provided remotely from multiple locations, meaning that the site where data is located and where the related services are performed is often different, subjecting users to unforeseen jurisdictions. Users need to be prepared for their service contract to dictate particular dispute resolution options. Additional risks apply to users who need to share data transnationally. Managing services over multiple jurisdictions is more difficult. Laws vary among jurisdictions and will apply differently depending in which nation the data is stored.

4. Users may lack certain recourse for lost data.

With one-sided contracts and a dearth of regulation, users may not be able to recover from service failures such as downtime and loss of data. Standard contracts often provide exceptions to the duty of care applied to providers. Many contracts will also have limited liability and/or limited remedies clauses. Courts have shown some willingness to enforce these clauses even though they heavily favor providers. See Trieber & Straub, Inc. v. UPS, Inc., 474 F.3d 379 (7thCir. 2007) (court upheld UPS' disclaimer of liability finding that UPS provided adequate notice to customers). If potential data damage and loss would be unusually detrimental to their business, users should try to negotiate actual damages for such an event.

5. Users cannot rely totally on insurance coverage for lost data.

Many insurance plans, which are intended to cover data loss and fraud, reduce or eliminate coverage if the data is stored on a Cloud. Users should check their policies before entering into Cloud service contracts.

6. Data stored on the Cloud may not be as secure as data on local servers.

Cloud remote access may expose companies to new privacy and security issues. With Cloud computing, users lose their ability to independently address security breaches. If a user is in a business that has mission-critical IT needs, then Cloud computing may not be worth the risks. In addition to users' own goals to keep data private, many users must comply with various laws that require data privacy, such as the Health Information Privacy Act and the Electronic Communications Privacy Act.

7. Managing Cloud contracts may present new compatibility challenges.

A lack of industry-wide data standards for transitioning between providers has damaged interoperability of data formats. Providers have an incentive to vary formats and prevent standardization because they can lock in customers to their own unique format. Compatibility with other systems is controlled by the provider, not the user. As a result, users may struggle to synch data with other provider platforms. Users should advocate for industry standardization.

8. Terminating a Cloud contract may not be easy.

Some providers have included a "data hostage" clause in their outsourcing contracts to discourage customer defections. When a customer seeks to terminate an outsourcing agreement, the provider demands payment in full or a

large termination fee. The service provider may simply hold the customer's data hostage until payment is made. One possible strategy to mitigate this risk is for users to seek shorter service contract durations and more favorable renewal terms. Another problem that arises at termination is the lack of interoperability among provider platforms which make transferring data to a new provider difficult and maybe impossible. In the negotiation stage, users should consider how to draft termination provisions that will minimize disruptions and develop a data transfer plan with their providers.

9. Data location and application ownership can be unclear.

With data stored and managed off-site and essentially controlled by the providers, locating the data and clarifying the role of the various service providers, namely, the hosts, can be problematic. Users should know where a copy of all stored data is physically located. Additionally, knowing how to access, audit, hold, and retrieve all data is critical. Certain regulations and e-discovery rules mandate particular data storage, protection, and transfer protocols and Cloud storage may not be permitted or compatible. Ready access is key. In addition to location, user ownership of data is critical to retain certain rights over the data and ensure confidential treatment. Providers should only own the hardware and not users' information. Providers often use subcontractors, who may not be readily known or liable to the user. Reliance on subcontractors affects data location and ownership issues.

10. Centralizing computing services in the Cloud can expose users to external risks.

Sharing resources may increase susceptibility to a single-point of failure in which a general outage is completely out of the Users' control. Aside from service interruptions due to outages or other failures, providers can automatically cut access to services if a bill goes unpaid. With large-scale providers, it can take hours or sometimes days to regain access. In light of these service interruptions, users should become acquainted with the providers' business continuity and disaster recovery practices. Users can also develop their own internal risk management strategies for these events.

The information in this Top Ten should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of its authors, its sponsors, and/or the ACC. This Top Ten is not intended as a definitive statement on the subject addressed. Rather, it is intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.

Reprinted with permission from the Association of Corporate Counsel (ACC)
2012 All Rights Reserved.

http://www.acc.com/legalresources/publications/topten/ttlrfccu.cfm