

## 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

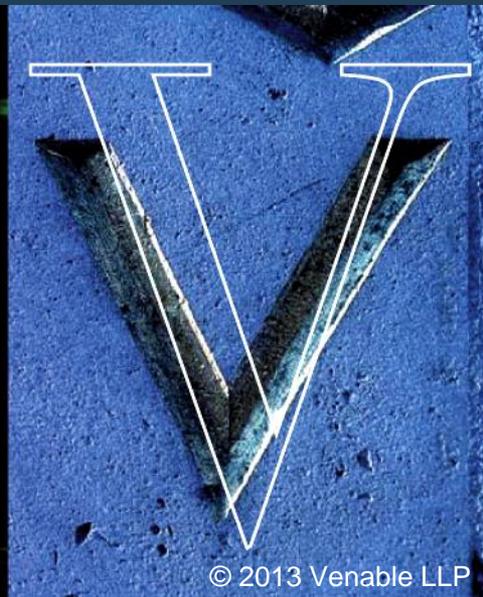
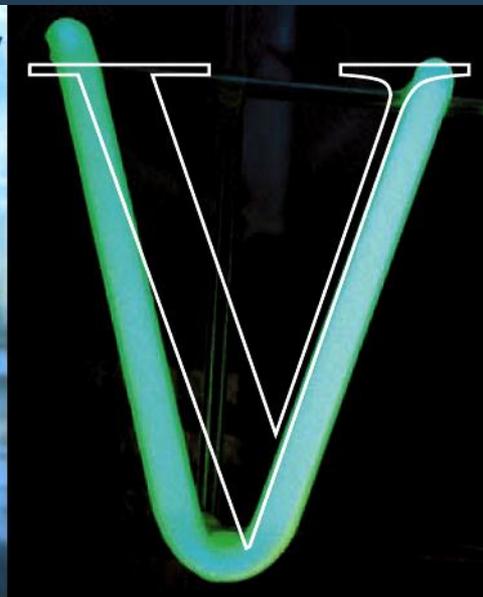
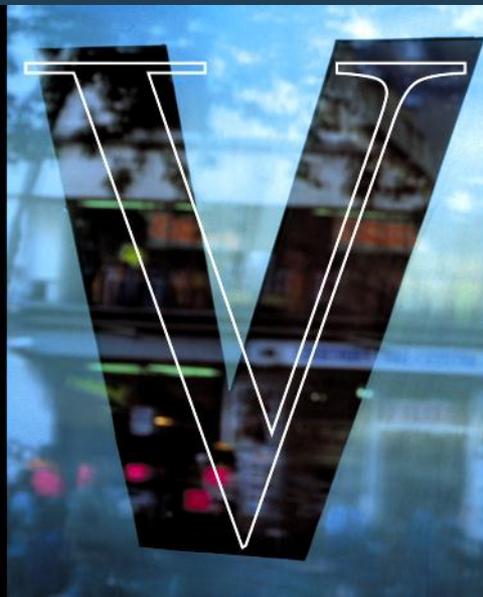
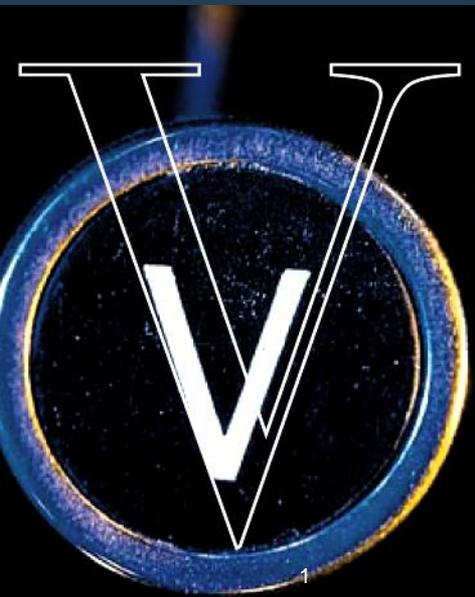
### Moderator:

Jeffrey S. Tenenbaum, Esq., Venable LLP

### Panelists:

A.J. Zottola, Esq., Venable LLP

Krista S. Coons, Esq., Venable LLP



## Upcoming Venable Nonprofit Legal Events

October 7, 2013 - [Association-Sponsored Market Research Programs: Common Pitfalls, Antitrust Risks, and Opportunities](#)

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

November 14, 2013 – Donor Intent, Restricted Funds, and Gift Acceptance Policies: What Every Nonprofit Needs to Know to Effectively Accept and Utilize Contributions (details coming soon)

December 5, 2013 – [Work & Family: What Nonprofit Employers Should Know about Family-Oriented Employment Laws](#)



# Agenda

- Apps
- The Cloud
- Information Security
- Electronic Contracting





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

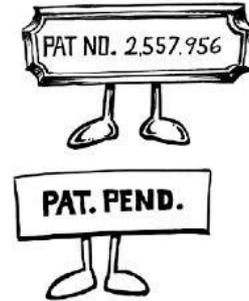
# But, What Exactly Is an App?



- 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



# Legal Considerations: IP for Apps



## ■ Copyright

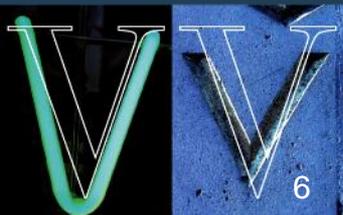
- Protects the tangible expression of the app itself, including its code, all words and images, and the audiovisual display (i.e., look and feel)

## ■ Trademark

- Protects all use of your company name, any logos, brands, product names, trade dress

## ■ Patent

- Protects inventive concepts



# 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!!



# 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



# Protecting Your IP

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



# 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.



# 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?



# 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



# 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?



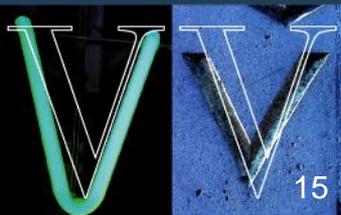


## What is the Cloud?

# 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.



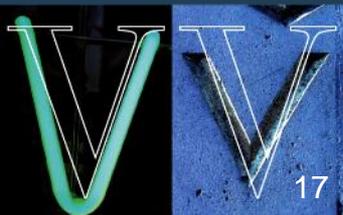
# Definitions of Deployment Models

- 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



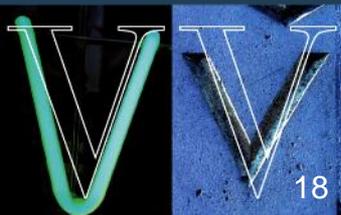
# Data Issues: Overview

- 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



## 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



## 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



# 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



## 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



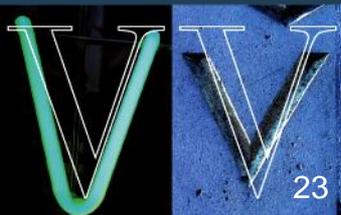
# In the Event of Litigation: E-Discovery Problems

- 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?



# 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



# 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

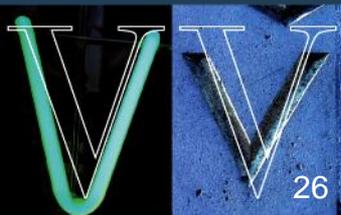


VENABLE<sup>®</sup><sub>LLP</sub>

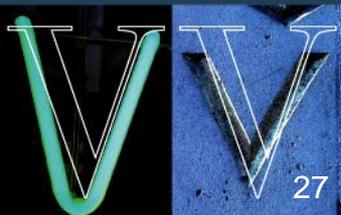
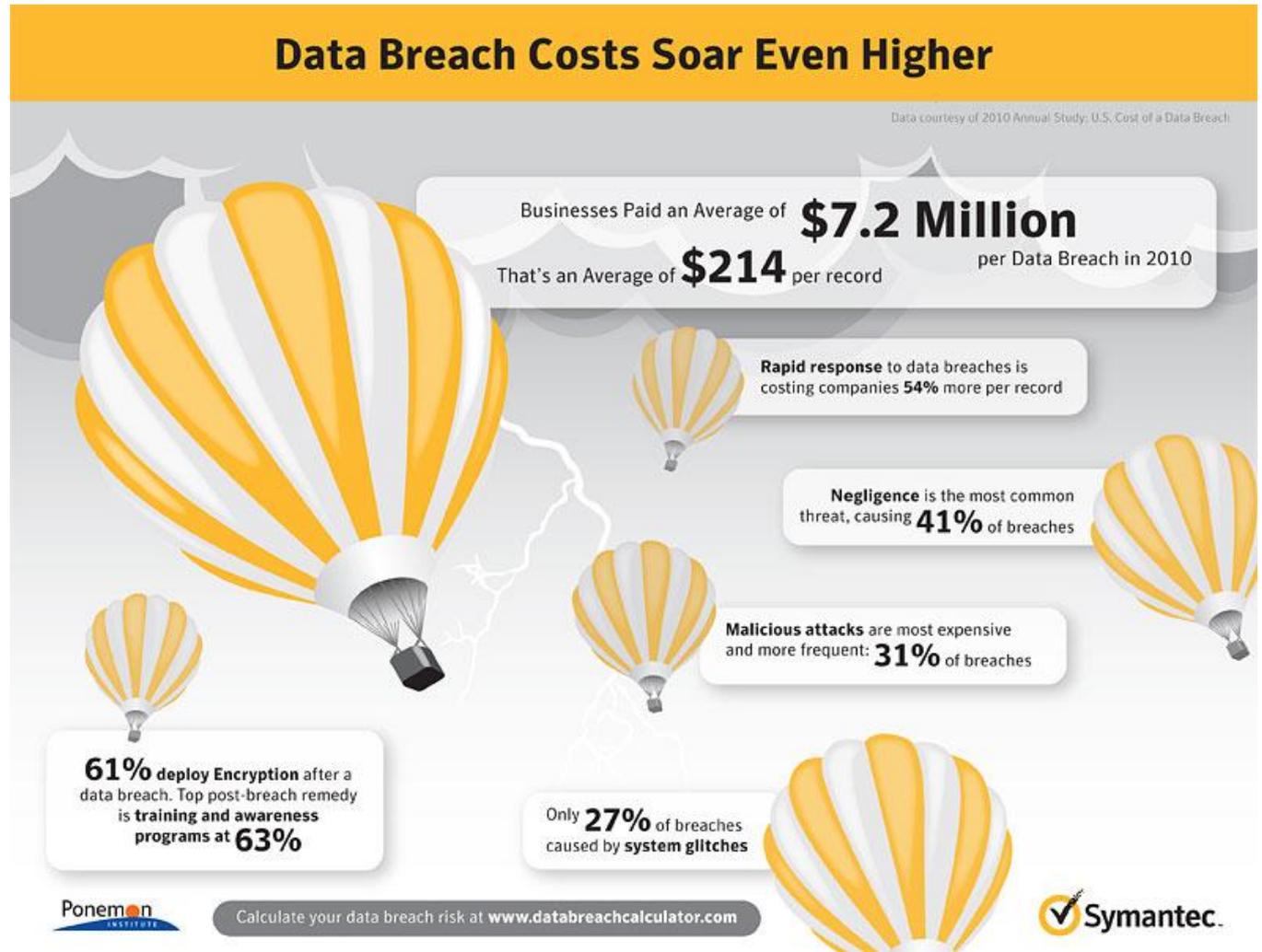
# Information Security

# 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

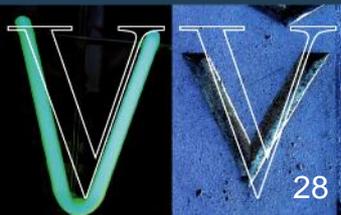
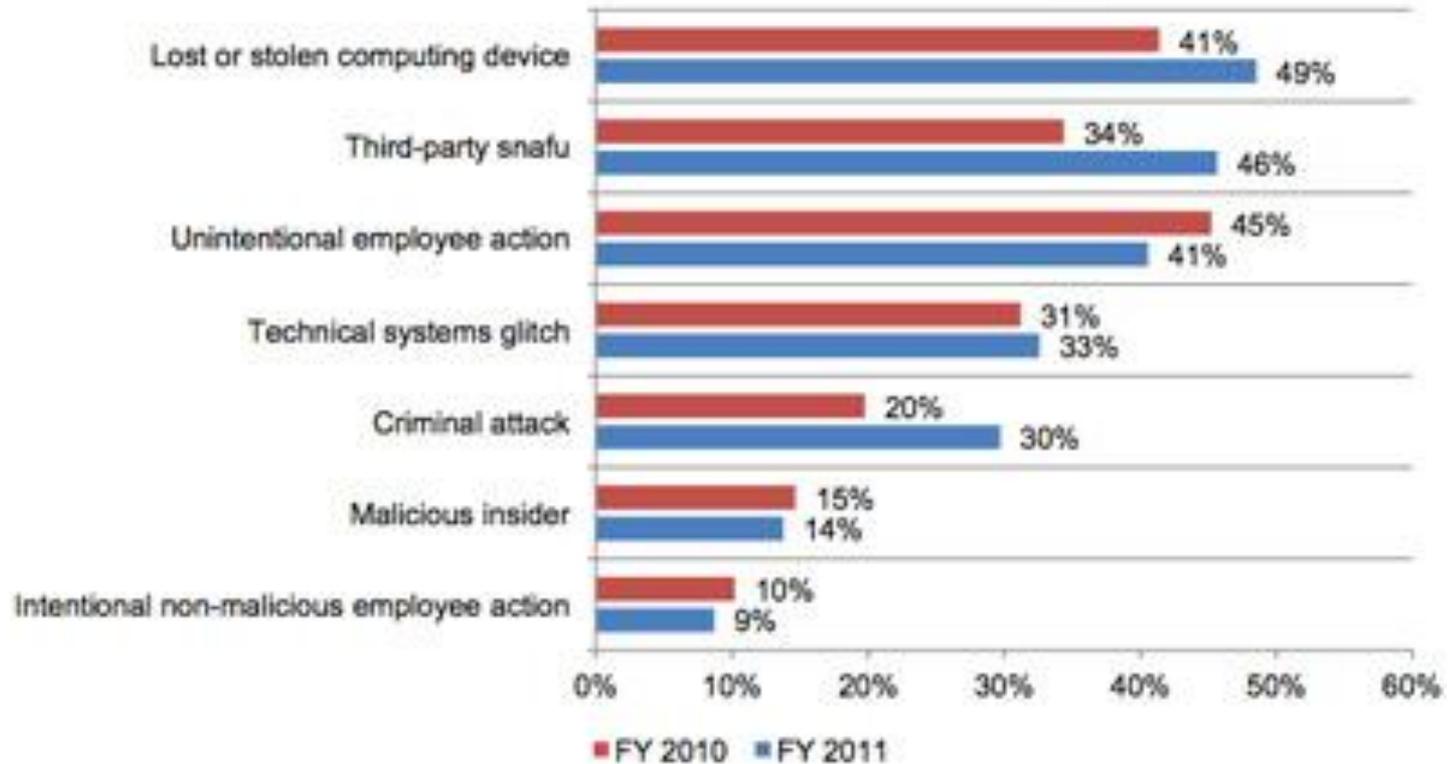


# Cost of Data Breach



# Employees, not hackers, cause most data loss

## Nature or root causes of the data breach incident



# 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



# 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



# 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



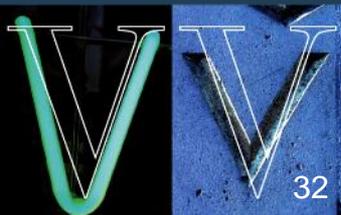
# Tactical Recommendations

<b>TACTICAL RECOMMENDATIONS (For Malware)</b>				
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

<b>TACTICAL RECOMMENDATIONS (For BYOD)</b>				
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



# 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



# Conclusion

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



VENABLE<sup>®</sup><sub>LLP</sub>

# Electronic Contracting

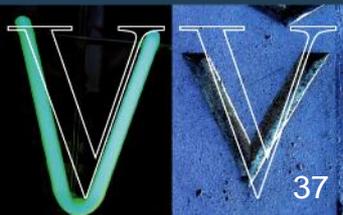
# Formation of a Contract

- Offer
- Acceptance
- Consideration



# 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



# 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



# 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



# Questions?

**Jeffrey S. Tenenbaum, Esq.**

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

t 202.344.8138

**A.J. Zottola, Esq.**

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

t 202.344.8546

**Krista S. Coons, Esq.**

[KSCoons@Venable.com](mailto: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](http://www.Venable.com/nonprofits/publications),

[www.Venable.com/nonprofits/recordings](http://www.Venable.com/nonprofits/recordings), [www.Venable.com/nonprofits/events](http://www.Venable.com/nonprofits/events).

