# Privacy and Data Security for Your Nonprofit: Understanding Your Legal Obligations and Insuring against Risk

August 13, 2014

Venable LLP

Washington, DC

*Moderator:*

Jeffrey S. Tenenbaum, Esq., Venable LLP

*Panelists:*

Emilio W. Cividanes, Esq., Venable LLP

Benjamin N. Beeson, Lockton Companies

# Presentation

# Privacy and Data Security for Your Nonprofit: Understanding Your Legal Obligations and Insuring against Risk

Wednesday, August 13, 2014, 12:30 p.m. – 2:00 p.m. ET
Venable LLP, Washington, DC

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

Panelists:
Emilio W. Cividanes, Esq., Venable LLP
Benjamin N. Beeson, Lockton Companies



## CAE Credit Information

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

As a CAE Approved Provider educational program related to the CAE exam content outline, this program may be applied for **1.5 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.*

*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.*

## Upcoming Venable Nonprofit Events

Register Now

September 16, 2014 – What's Ahead for 2015: Preparing Your Nonprofit's Group Health Plan for the Employer Mandate





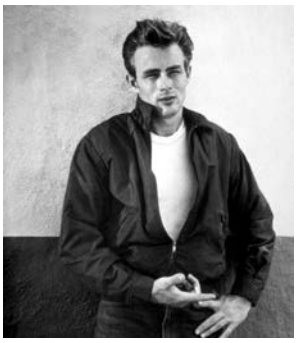
## Agenda

- The Cyber Threat Landscape
- Top 4 Risks to Nonprofits
- Risks Are Getting Riskier…
  - Part 1: Top 4 Industry Trends
  - Part 2: Top 4 Legal Developments
- Ten Steps to Mitigating Privacy and Data Security Risks
- Cyber Insurance
- Cyber Risks on the Horizon

# The Cyber Threat Landscape



## Four Horsemen of the “Cybocalypse”




# What's the "Catch"?

## Information Targeted by Attackers

| Category | Objective | Examples |
|---|---|---|
| Financial | Personally Identifiable Info | Identity Theft Or Inadvertent Loss |
| | ATM Withdrawals | RBS Worldpay $9.3M |
| | Payment Card Data | TJX, Hannaford, Heartlands |
| | ACH Transactions | Finance Person Targeted |
| Intelligence | Intellectual Property | Corporate Misdeeds |
| | Corporate Strategy | Senior Exec E-Mail |
| | Attorney/Client Comm | Gipson Hoffman & Pancione |
| | R&D Material | Many Industries |
| | Government Plans | Democratic Nat'l Committee |
| | Military Secrets | F35 Lightning Fighter Jet |
| | Energy Infra Architecture | Rumored Data Collection |
| Other | Destruction/Disruption/Leaks | Insiders, Hacktivists |





# But I'm Just a Nonprofit…What Do I Have to Fear?

TECHNOLOGY | NYT NOW

**Russian Hackers Amass Over a Billion Internet Passwords**

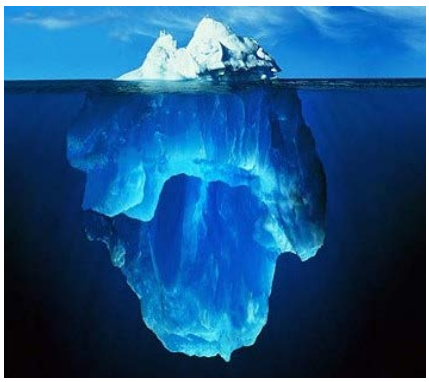
By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

# Top 4 Risks to Nonprofits



## Financial Costs of a Data Breach



- Forensic consultants
- Lawyers
- Call centers
- Credit monitoring
- Public relations crisis response and repair

## Reputational Damage

- Front page news
- Notifying donors, employees, consumers, government agencies
- Public outcry
- Erosion of donor trust
- Antipathy of service constituency; boycotts


**Data breach at Indiana University may affect 146,000 students**

February 26, 2014 | Reuters

StarTribune

**Goodwill, feds investigate possible data breach**

Associated Press
July 22, 2014 - 11:27 AM





## Government "Fine"-Tuning

- Watchdogs have a lot to watch in today's nonprofit world:
  - Electronic solicitations (CAN-SPAM)
  - Donation platforms (breach laws)
  - Donor list management (privacy policies)
  - Social media outreach (COPPA)

- Government handing out fines to nonprofits

**Md. nonprofit serving disabled reports data breach**

By DAVID DISHNEAU - Associated Press - Monday, March 17, 2014

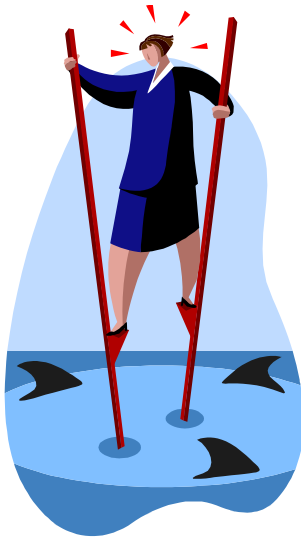
For Immediate Release - July 23, 2014

**Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients**

Hospital Allegedly Failed to Protect Personal Information and Protected Health Information of More Than 12,000 Massachusetts Patients

## A Not-So-Class Act: More Privacy/Data Security Lawsuits

- Organizations have been sued for:
  - Failing to maintain reasonable data security
  - Collecting personal information with payment
  - Sharing data with third parties
  - Mobile device practices







# Risks Are Getting Riskier…

## Part 1: Top 4 Industry Trends

## Data Collection: Turn up the Volume of Data Flow

- Online giving: fastest growing fundraising channel for nonprofits
- Social media: key to donor and constituent engagement
- Move to mobile and "internet of things": geolocation and more






## The Growing Uses of Data: More of It, More from It


- Big Data: Opening the door for analytics and predictive modeling
  - Boost donor network and fundraising opportunities
  - Extend reach of services and solicitations
  - Develop new products and services

## Data Transfer and Storage: All Systems Cloud and Clear

- Nonprofits gain from hosted IT services and cloud-based solutions that cut costs and free up resources.
- More vendors means more third-party access to data.

- Data sharing fosters collaboration within and beyond the organization.





## The Growing Value of Data

1994

2014

- Data revolution driving all decision-making for entities and individuals alike
- Growing dependence on data boosts ROI for cybercriminals

# Risks Are Getting Riskier…

## Part 2: Top 4 Legal Developments



## Legislative and Enforcement Push after High Profile Breaches


## Security Standards for a New World

- Data security
  - Duty of care: Be **REASONABLE**
- Cyber security
  - NIST framework for ***critical infrastructure***
  - *De facto* standard of care for everyone else?
- Preparation
  - Incident response planning a must





## State Government Watchdogs: Lots of Bark and Lots of Bite

- Innovation means new practices
- New practices mean more scrutiny
- Privacy policies, terms of use, types of data

## Expect the Unexpected: The Evolving Privacy Landscape

- Government surveillance revelations driving public sensitivities


- Expansion of PII (geolocation, biometric) transforming nature of privacy





## Summary

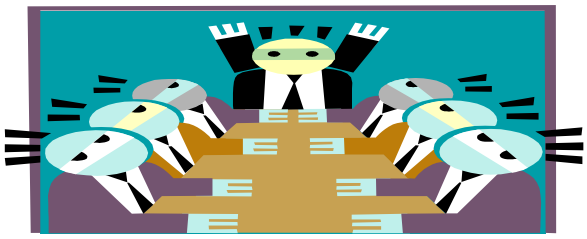
- Top 4 Risks to Nonprofits
  - Cost of a breach
  - Reputational damage
  - Government fines
  - Class action lawsuits
- Risks Getting Riskier: Industry Trends and Legal Developments
- Top 4 Industry Trends
  - Data collection; use; transfer/storage; value
- Top 4 Legal Developments
  - Legislative/enforcement push; data/cyber standards; UDAP enforcement; shifting expectations of privacy

# Ten Steps to Mitigating Privacy and Data Security Risks



## Ten Steps to Mitigating Privacy/Data Security Risks: #1

1) Accept that this is an enterprise-wide risk, not just an IT issue.
   - Stakeholders include but are not limited to the Boardroom, HR, Audit, IT and Legal.



## Ten Steps to Mitigating Privacy/Data Security Risks: #2

2) Establish technical expertise in or reporting to the board.
   - This is primarily a governance issue that must be addressed from the top down in any organization.
   - Establish a line of sight into the board, translating in layman's terms both technical and legal jargon.





## Ten Steps to Mitigating Privacy/Data Security Risks: #3

3) Identify your organization's most critical data assets.
   - Where do these assets reside?
   - Who has access to these assets?

## Ten Steps to Mitigating Privacy/Data Security Risks: #4

4) Identify vendors used for business functions involving critical data assets.
   - Seek to transfer risk contractually.
   - Understand where data is stored.
   - Understand the level of vendor security.
   - Require vendor to buy cyber insurance.





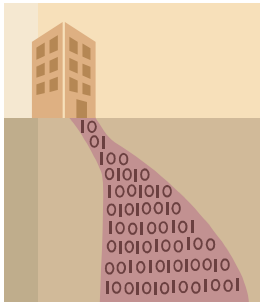
## Ten Steps to Mitigating Privacy/Data Security Risks: #5

5) Defense in depth – assume attackers will penetrate your network.
   - Firewalls to protect perimeter
   - Intrusion detection systems
   - Two factor authentication
   - Anti-virus
   - Encryption

## Ten Steps to Mitigating Privacy/Data Security Risks: #6

6) Encrypt portable devices.

- Payroll PHI or PII
- Customer PHI or PII
- Corporate confidential information







## Ten Steps to Mitigating Privacy/Data Security Risks: #7

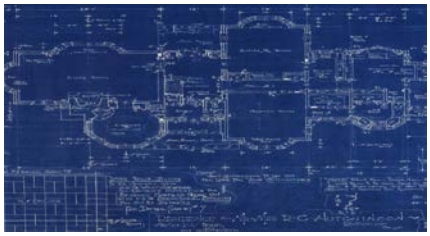
7) Understand your legal obligations.

- PCI DSS – Credit card data
- HIPAA – PHI
- State data breach laws – PII / PHI
- FTC – Privacy policy
- EU – Cookies consent

## Ten Steps to Mitigating Privacy/Data Security Risks: #8

8) Establish a data breach incident response plan.

- Identify the legal department as quarterback.
- Establish a reporting structure to legal.
- Set up key legal, IT, forensic, and PR vendor relationships.



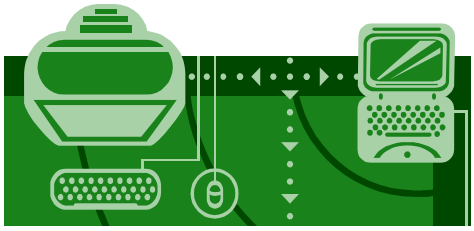




## Ten Steps to Mitigating Privacy/Data Security Risks: #9

9) Consider an intelligence-led approach on security.

- Active network monitoring
- Understand who your attackers are and what they want.



## Ten Steps to Mitigating Privacy/Data Security Risks: #10

10) Consider buying cyber insurance.

WHY?

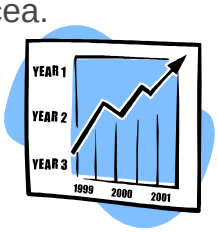




# Cyber Insurance

## Why Buy Cyber Insurance?

- Despite your best efforts to mitigate, it is impossible to prevent a breach. This is about resilience.
- You are liable in the event of a vendor breach of your employee or customer PII or PHI. Insurance will address.
- PCI DSS compliance is not a panacea.
- Balance sheet protection








## What Does Cyber Insurance Cover?

- Data breach response costs

Notification
IT Forensics
Public Relations
Credit Monitoring

## What Does Cyber Insurance Cover?

- Privacy regulatory action

Defense costs and civil fines from a regulator such as the FTC or state attorney general.





## What Does Cyber Insurance Cover?

- Civil litigation

Defense costs and damages from a civil action – class action from employees or customers, for example.

## Top Ten Questions to Ask Your Broker

1) How much insurance should I buy?
2) Which insurance carriers do you recommend and why?
3) Does the insurance carrier require you to use their own vendor panel or not? If so, who are these vendors, and what is their experience?
4) Are you able to use your own outside counsel in the event of litigation? If so, does the insurer still seek to cap the hourly rate?
5) What is the claims experience of the carrier?




## Top Ten Questions to Ask Your Broker

6) How does the policy form define personal data?
7) Are there any privacy exclusions such as wrongful collection of data or unsolicited email?
8) Are data breach response costs sublimited?
9) Is there any limitation on coverage for vicarious risk to vendors?
10) Is knowledge and notice of a claim restricted to the executive team?

## State of the Insurance Market

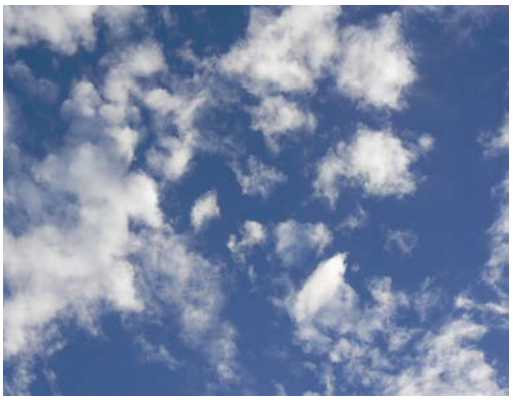
- Over $1 billion in gross written premiums
- $350,000,000 total insurance capacity
- Approximately fifty insurers between the US and London insurance market underwriting data security and privacy risk
- All policy forms are not the same
- Indemnity versus vendor approach





## Cyber Risks on the Horizon

- "Internet of Things" – Property damage and bodily injury
- Big Data
- The Cloud



# Questions?

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

**Emilio W. Cividanes, Esq., Venable LLP**
ewcividanes@Venable.com
t 202.344.4414

**Benjamin N. Beeson, Lockton Companies**
bbeeson@lockton.com
t 202.414.2400

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

To view recordings of Venable's nonprofit programs on our YouTube channel, see www.youtube.com/user/VenableNonprofits.

# 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, 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 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 selected for inclusion in the 2014 edition 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.

## AREAS OF PRACTICE

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

## INDUSTRIES

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

## GOVERNMENT EXPERIENCE

Legislative Assistant, United States House of Representatives

## BAR ADMISSIONS

District of Columbia

## REPRESENTATIVE CLIENTS

AARP
Air Conditioning Contractors of America
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 Institute of Architects
American Society for Microbiology
American Society for Training and Development

## 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

American Society of Anesthesiologists
American Society of Association Executives
America's Health Insurance Plans
Association for Healthcare Philanthropy
Association of Corporate Counsel
Association of Fundraising Professionals
Association of Private Sector Colleges and Universities
Auto Care Association
Biotechnology Industry Organization
Brookings Institution
Carbon War Room
The College Board
CompTIA
Council on CyberSecurity
Council on Foundations
CropLife America
Cruise Lines International Association
Design-Build Institute of America
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 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
Telecommunications Industry Association

Trust for Architectural Easements
The Tyra Banks TZONE Foundation
U.S. Chamber of Commerce
United Nations High Commissioner for Refugees
Volunteers of America

## HONORS

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.), 2012-14

Selected for inclusion in *Washington DC Super Lawyers*, Nonprofit Organizations, 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.

VENABLE® LLP

our people

# Emilio W. Cividanes

Partner

Washington, DC Office

T 202.344.4414 F 202.344.8300

ecividanes@Venable.com

Emilio Cividanes concentrates his practice on helping companies meet their privacy obligations in a competitive and global marketplace, and shape the data protection laws and regulations that govern their activities. His practice centers on counseling clients in various industries, including marketing, entertainment, electronic publishing, telecommunications, retail, health care, pharmaceutical, financial services, and hospitality, on how to address privacy challenges to their product development, sales, and other business operations.

## AREAS OF PRACTICE

Communications

Legislative and Government Affairs

Advertising and Marketing

Advertising and Marketing Litigation

Homeland Security

Appellate Litigation

Technology Transactions and Outsourcing

Privacy and Data Security

Congressional Investigations

Healthcare

Class Action Defense

Litigation

Consumer Finance

Regulatory

## INDUSTRIES

Financial Services

Consumer Products and Services

Consumer Financial Protection Bureau Task Force

Cybersecurity

## GOVERNMENT EXPERIENCE

United States Senate, Judiciary

## SIGNIFICANT MATTERS

In servicing his clients, which range from Fortune 100 companies to start-ups, Mr. Cividanes has:

- Counseled clients on how to minimize the risk of personal data security breaches and mitigate the risks when they occur;
- Lobbied Congress and federal agencies, and participated in the drafting of virtually every federal privacy regulation implemented during the past ten years;
- Advised companies on how to structure their business models, employment practices, and corporate acquisitions to reduce the burden of complying with privacy regulations;
- Performed audits of companies' practices to help management or potential acquirers assess the companies' compliance with relevant laws, regulations, and self-regulatory programs;
- Counseled Internet and telecommunications service providers, and cable TV operators, on compliance with federal and state wiretap laws;
- Advised domestic companies with operations abroad on compliance with requirements for the transfer of personal data from Europe to the United States;
- Drafted privacy policies that meet regulatory or self-regulatory requirements;
- Assisted trade associations and other business groups to develop self-regulatory standards, including compliance questionnaires, and privacy policy generators or wizards;
- Advised private companies involved in government contracts on compliance with the Privacy Act; and
- Counseled clients on privacy issues arising from contracts and transactional negotiations.

Mr. Cividanes has also:

- Defended clients that are the targets of class action suits alleging violations of privacy laws;
- Represented clients in "crisis mode" because of unwanted scrutiny from the

Committee, Subcommittee on Technology and the Law

## BAR ADMISSIONS

District of Columbia

## EDUCATION

J.D., University of Pennsylvania Law School, 1983

Comment Editor, *Pennsylvania Law Review*

B.A., Haverford College, 1979

Federal Trade Commission, the Congress, or the National Advertising Division of the Council of Better Business Bureaus; and

- Challenged privacy regulations in court and filed "friend of the court" briefs in landmark cases.

## HONORS

Recognized in *Chambers Global*, Privacy and Data Security, 2011–2014

Recognized in *Chambers USA*, (Band 2), Privacy and Data Security, National, 2008–2014

Recognized in *Legal 500*, Technology: Data Protection and Privacy, 2010–2014

Recognized in *Super Lawyers Business Edition*, Business/Corporate, Washington, DC, 2013

Selected for inclusion in *District of Columbia Super Lawyers*, 2012 and 2013

AV® Peer-Review Rated by Martindale-Hubbell

## ACTIVITIES

Mr. Cividanes has taught information privacy law as an adjunct professor at Georgetown University Law Center, and served as counsel to the Technology and the Law Subcommittee of the U.S. Senate Judiciary Committee. Mr. Cividanes is a Fellow of the American Bar Foundation and has served as a member of the Board of Trustees of the Public Defender Service for the District of Columbia and a member of the Board of Directors of the Hispanic Bar Association of the District of Columbia.

## RECENT PUBLICATIONS

- June 2014, The Download - June 2014, The Download
- February 2014, The Download - February 2014, The Download
- November 2013, The Download - November 2013, The Download
- October 2013, The Download - October 2013, The Download
- August 2013, The Download - August 2013, The Download
- June 2013, The Download - June 2013, The Download
- May 2, 2013, Redial Unsuccessful - TCPA Claims Still Unavailable in New York, Class Action Alert
- March 29, 2013, Advertising News & Analysis - March 28, 2013, Advertising Alert
- March 2013, Telemarketers Dial Quickly - TCPA Class Action Dismissed For Now, Class Action Alert

## RECENT SPEAKING ENGAGEMENTS

- August 13, 2014, Privacy and Data Security for Your Nonprofit: Understanding Your Legal Obligations and Insuring against Risk
- May 6, 2014, CLE on "Video Privacy Protection Act"
- December 4, 2013, "Insights from FTC Privacy Investigations: Do's and Don'ts" for IAPP's Practical Privacy Series
- March 21, 2013, "Managing Cybersecurity Risks for Financial Institutions" for ALI CLE

**Benjamin N. Beeson**

Vice President
Cyber Security and Privacy
Lockton
bbeeson@lockton.com

Ben Beeson is Vice President for Cyber Security and Privacy at Lockton. Based in Washington, D.C., Ben joined Lockton in 2007 and only recently relocated to the United States from London, where he led the global cyber risk practice. He is known as a cyber risk thought leader in the commercial insurance market, and has been at the forefront in supporting U.S. and U.K. government efforts to improve industry resilience to cyber attacks.

# Additional Information

# Evolving Cyber Threats

## Can the Insurance Market Respond?

July 2014 • Lockton® Companies

### In the Beginning

**BEN BEESON**
Vice President
Producer
202.414.2653
bbeeson@lockton.com

The emergence of the Internet as a business platform at the end of the nineties also announced the arrival of new risks to organizations. In those early days, there was a widely held belief that the primary concern was operational, amidst concerns about the impact of a computer virus or the actions of a "hacker," a new term to many of us then.

Despite the lack of actuarial data, a few underwriters in the U.S. and London started to devise solutions to indemnify business interruption losses and the costs to restore compromised data. Commonly known as "Hacker Insurance," we found few buyers beyond large U.S. banks. Clients found the underwriting process both intrusive and expensive as insurers demanded on-site security audits.

On July 1st 2003 everything changed.

California enacted SB 1386, the world's first data breach notification law. Industry had started to understand that the Internet would revolutionize the way that it could store and use data, especially personal information on its customers. However, government and regulators also started to appreciate that this new opportunity could be open to significant abuse and, as the majority of U.S. states started to enact their own data breach notification laws, the risk evolved into a privacy issue.

LOCKTON®

During the next ten years, insurers responded by developing solutions to address the risks of handling customer, employee, and patient personal information from either unauthorized disclosure or a violation of privacy. Today, it is estimated that the total gross written premium exceeds $1 billion with $350 million in total capacity. However, the threat is changing, and the issue for many organizations is moving back to where it started: an operational risk.

While we are coming full circle, this time it is different.

Why?

## Moving Beyond Stuxnet

You may be familiar with the Stuxnet virus. Stuxnet is widely regarded as the world's first cyber weapon. In 2010, it came to light that a sophisticated attack had damaged Iranian nuclear centrifuges. Significantly, this provided evidence that physical damage could now be caused by a cyber attack.

Stuxnet, perhaps unsurprisingly, has stolen the limelight, but in many respects it has had a negative impact in helping boards understand the risk that they are facing. There is no doubt that education and awareness are factors, but many organizations simply viewed Stuxnet as a one-off event with little or no relevance to their own security program.

However, companies face real, tangible operational risks from a cyber attack today that could cause physical damage, business interruption, or bodily injury.

According to Mandiant, a FireEye Company, 95 percent of Advanced Persistent Threats (APTs) are caused by spear phishing, typically an individual opening an email from who they think is a trusted third party. Opening the email allows the perpetrator to install malware on the user's network and then connect to a command and control server. That's all it takes. Once in, the perpetrator will move laterally across the network looking for what he or she wants.

The advent of APTs raise significant questions about the whole approach to enterprise cyber security. Many CIOs and CISOs have typically set up a "defense in depth" strategy protecting the perimeter with a firewall, intrusion detection systems, antivirus software, encryption, and other tools.

However, many attackers increasingly use "zero days," meaning previously unknown vulnerabilities, thereby rendering signature-based defenses redundant (or irrelevant?).

If you are a board member or executive, you should worry about APTs, not Stuxnet. This threat has also started to concern governments worldwide.

Commercial espionage and data security and privacy capture many headlines. But sabotage, particularly on critical infrastructure industries, is now a serious threat. Enterprises in energy, transportation, financial, healthcare, and manufacturing industries, amongst others, face the biggest operational risk challenges from a cyber attack. Some of these industries are particularly vulnerable as they use operational technology such as SCADA systems that are increasingly connected to corporate IT networks.

> "The operational risks from a cyber attack today causing physical damage, business interruption, and bodily injury could not be more real."

## The NIST Cyber Security Framework

Government concern has not yet translated into legislation forcing industry to improve its resilience and security posture.

In the U.S., President Obama issued Executive Order 13636 in 2013 tasking the National Institute of Standards and Technology (NIST) with developing a cyber security framework. The insurance industry has reacted very positively, seeing a partnership emerging with government to start to address previously uninsurable risks. The industry was a key stakeholder in the creation of the framework and is now working with the Department of Homeland Security in its implementation. Other countries are looking to follow a similar approach to the U.S.. The U.K. government recently announced its Cyber Essentials scheme focused more on smaller businesses rather than critical infrastructure industries.

Although voluntary, many legal commentators feel that the new framework will lead to an increase in risk to boardrooms. A benchmark now exists that shareholders could reference in the event of a major cyber attack. In addition, and perhaps without realizing it, by directly engaging the insurance industry, the government has done the industry as a whole a great favor. Insurers are being forced to confront questions about risks and coverage that had not previously been asked, and they are starting to receive some uncomfortable answers.

## Am I Insured?

Specialist insurance policies to address data breaches and privacy violations are well understood. Theft of corporate intellectual property from a cyber attack is also commonly known to be a risk that insurers have yet to understand how to address.

However, and particularly in the context of attacks on critical infrastructure industries, there is a great deal of ambiguity for losses involving physical damage, bodily injury, or business interruption. Don't my property or commercial general liability policies address this? At best, the answer is maybe. Some policies will specifically exclude, some will provide limited coverage, whilst others will be silent. Considering the nature of the threat and the potential impact on the organization, silence can no longer be acceptable, and affirmative insurance policy language is a must.

The good news is that the industry is already starting to respond. Two insurers to date have announced a "Difference in Conditions" (DIC) approach, overlaying the gaps that exist in the property and general liability forms. Another has launched a terrorism policy to also address cyber attacks. This is all positive but it is just the start. Insuring the risks is one thing, but building out significant capacity to ensure coverage is worth buying is also vital.

Over the coming months and years, insurers will start to work more closely with both government and the security industry. Just as enterprises start to realize that they must change their approach to security from defense-in-depth to an intelligence-led strategy, so insurers will partner with security firms to adapt their underwriting approach on the same basis.

Understanding who is trying to attack you and what they want, aligned with informed decision makers in or reporting directly to the board, will be key.

About the author:

Ben Beeson, a British national, recently relocated from London to Washington, D.C., where he is a leader in the Cyber Security Practice for Lockton Companies.

## Our Mission

To be the worldwide value and service leader in
insurance brokerage, employee benefits, and risk management

## Our Goal

To be the best place to do business and to work

www.lockton.com

VENABLE LLP

# the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY



ISSUE EDITORS

**Stuart P. Ingis**
singis@Venable.com
202.344.4613

**Michael A. Signorelli**
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

**Emilio W. Cividanes**
ecividanes@Venable.com
202.344.4414

**Tara Sugiyama Potashnik**
tspotashnik@Venable.com
202.344.4363

**Julia Kernochan Tama**
jktama@Venable.com
202.344.4738

**Kelly A. DeMarchis**
kademarchis@Venable.com
202.344.4722

**Ariel S. Wolf**
awolf@Venable.com
202.344.4464

**Robert L. Hartwell**
rlhartwell@Venable.com
202.344.4663
www.Venable.com

February 2014

## In this Issue:



## Heard on the Hill

### Congress Holds Hearings on Preventing Data Breaches

In the aftermath of recent data breaches, the Senate Banking, Housing, and Urban Affairs' Subcommittee on National Security and International Trade and Finance, the Senate Judiciary Committee, and the House Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade conducted a series of hearings to examine potential solutions to prevent data breaches in the public and private sector.

Members of Congress and witnesses present at these hearings considered various tools to help prevent data breaches or otherwise respond to data breaches, including the expansion of the Federal Trade Commission's ("FTC") authority to regulate and enforce data security and breach notification measures and increased penalties on companies that knowingly conceal a breach. During and after these hearings, several members of Congress have announced their support for broad adoption of the "Chip and PIN" system to replace technologies that are more widely

used at point of sale ("POS") systems in the United States.

### Senate Banking Subcommittee on National Security and International Trade and Finance

On February 3, 2014, the Senate Banking, Housing, and Urban Affairs' Subcommittee on National Security and International Trade and Finance ("Subcommittee") convened a hearing on data breaches entitled, "Safeguarding Consumers' Financial Data." The Chip and PIN system was repeatedly discussed throughout the hearing as a potential technology solution to help prevent hackers from obtaining unauthorized access to personal information from POS systems. Subcommittee Chairman Mark Warner (D-VA) stated his support for the Chip and PIN system, calling on the card industry and retailers to adopt the system.

### Senate Judiciary Committee

On February 4, 2014, the Senate Judiciary Committee ("Committee") held a hearing on data breaches entitled, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." Senators present at the hearing agreed that recent data breach occurrences at retailers demonstrate a systemic issue that can only be addressed through collaboration from stakeholders and the government. During the hearing, Judiciary Chairman Patrick Leahy (D-VT) sought to draw support for his legislation, S. 1897, the Personal Data Privacy and Security Act of 2014. Senator Richard Blumenthal (D-CT) promoted his legislation, S. 1995, the Personal Data Protection and Breach Accountability Act of 2014.

### House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade

On February 5, 2014, the House Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") held a hearing on data breaches entitled, "Protecting Consumer Information: Can Data Breaches Be Prevented?". Unlike the two Senate hearings on the same subject held earlier during the same week, this hearing waded into privacy issues as well. Representative Joe Barton (R-TX), Co-Chair of the Bi-Partisan Privacy Caucus ("Caucus"), stated that results from the hearing will supplement discussions in future Caucus meetings on such issues. Similarly, Representative Marsha Blackburn (R-TN) and Representative Peter Welch (D-VT), Co-Chairs of the Privacy Working Group ("Group"), noted that issues raised during the hearing will contribute to the dialogue during future Group meetings.

## Around the Agencies

### The NTIA Multistakeholder Process Continues

On February 6, 2014, the National Telecommunications and Information Administration ("NTIA") commenced a new multistakeholder process focused on facial recognition technology. Like the earlier NTIA multistakeholder process, which began in 2012 and focused on mobile application transparency, the purpose of the initial February meeting was to begin to develop a voluntary, enforceable code of conduct designed to provide transparency related to the use of facial recognition technology.

This meeting is the first of eight scheduled through June 2014.

Lawrence Strickling, Assistant Secretary for Communications and Information and Administrator of NTIA kicked off the meeting with remarks about the process' goal, which is to facilitate discussion on a path forward applying the White House's Consumer Privacy Bill of Rights to facial recognition technology in the commercial context.

The meeting featured three panels focused on the fundamentals of facial recognition technology, its commercial applications, and technical privacy safeguards.

The first panel featured panelists who provided information about the accuracy of the technology, and how it is currently applied, especially as used to determine age, gender, race, ethnicity, sexual orientation, and emotion. Audience questions probed the panel about the accuracy of matching photos to a database.

The second panel, which focused on marketing research and commercial applications of the technology, focused on its many positive uses. They explored how in marketing facial recognition technology can be used to gauge concepts such as emotional response, as well as improve accuracy by authenticating marketing participants. Other commercial applications touched upon were security and law enforcement. The audience focused on the use and sharing of this data.

Finally, the third panel discussed privacy safeguards over the data, including the risks arising from the linkage of offline data with online profiles. The audience focused on how notice would be provided to individuals about the use of facial recognition technology, as well as the limits of this technology and its potential for misuse.

On February 25, 2014, NTIA convened a second meeting of the facial recognition multistakeholder process. At this meeting, NTIA stressed that the process was focused on issues related to commercial use with the objective of drafting a private code of conduct. Facial recognition industry experts presented on key aspects of the technology, such as algorithms used to generate biometric templates and the error rates associated with the technology. During the facilitated discussion, participants discussed the size of databases used for matching as well as various factors that contribute to accuracy. At the end of the meeting, NTIA and participants agreed to conduct additional fact-finding at the next meeting in March, to be followed by an effort to begin drafting a code of conduct.

## Department of Commerce Reports on U.S.-EU Safe Harbor Discussions

A delegation from the Department of Commerce ("Commerce") recently traveled to Brussels, Belgium to discuss the U.S.-EU Safe Harbor program with their European counterparts. The meetings centered on the thirteen recommendations for the Safe Harbor program issued by the European Commission ("EC") in a November 2013 report.

Commerce staff reported that the meetings focused mostly on the first eleven recommendations dealing with transparency, consumer redress, and enforcement, and did not delve deeply into the national security issues raised by the recommendations.

A series of meetings are being planned by Commerce to discuss all the recommendations, but with a greater focus placed on national security issues. These meetings are planned for Washington, D.C. through the spring.

### FTC Holds Seminar on Mobile Device Tracking

On February 19, 2014, the Federal Trade Commission ("FTC") hosted a seminar entitled, "Mobile Device Tracking," as part of its Spring Privacy Series on emerging consumer privacy issues. The seminar included a panel of industry and consumer group experts on the emerging practice of device tracking. The panel covered the technical, legal, and policy challenges that will confront consumers and businesses in this new field.

After a presentation about the technology behind device tracking, questions about how retailers and marketers use the information gained from mobile devices were posed to the panel. The panel described various business and customer facing uses for the data, including faster checkout times, more efficient inventory management, and better theft prevention. The results of a recent study of consumer feelings toward sharing location data in exchange for deals or coupons was also released at the seminar, finding that 97 percent of Americans are willing to make such an exchange.

The seminar concluded with questions regarding the privacy implications of device tracking and the need for consumer notice. A distinction was made between app specific information and location data gathered from a device's antenna. Panelists discussed how device tracking companies collect information from the antenna, and not specific information from device applications. The panel cautioned against over-notification, and stressed the need to focus on the use of the collected data, not solely on how the data is collected. The FTC is expected to continue to study this space.

## White House Developments

### White House and NIST Release Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity

On February 12, 2014, the White House launched version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). The Framework was developed by the National Institute of Standards and Technology ("NIST") pursuant to Executive Order 13636, signed by President Obama in February 2013. The Framework was prepared in collaboration with industry stakeholders, and is presented as a guide to aid critical infrastructure companies in establishing and improving their cybersecurity programs.

The Framework closely tracks the draft that was released in October 2013. As with the earlier version, the Framework is still composed of the Framework Core, Profiles, and Implementation Tiers. Each component includes NIST recommendations for how to use and integrate the components and standards into a cybersecurity program.

One major change in the Framework is that the appendix discussing privacy and civil liberties has been integrated into a "Methodology to Protect Privacy and Civil Liberties" in the "How to Use" section of the Framework. Regarding the protection of civil liberties arising from cybersecurity activities, "direct responsibility" is limited to "government or agents of the government." As to "privacy implications," the Framework directs organizations to consider how a cybersecurity program "might incorporate privacy principles" such as data minimization, use limitations, individual consent and redress, and accountability. The Framework provides a list of processes and activities that may be considered as a means to address these principles. The announcement of the Framework was accompanied by the release of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity ("Roadmap"). The Roadmap provides a vision of how NIST hopes to improve the Framework overtime.

NIST will also begin the process of developing a privacy risk management model and technical standards. The goal of this process will be to identify and develop technical standards or best practices to mitigate the impact of cybersecurity on individual privacy. To begin this process, NIST will hold a privacy workshop in the second quarter of 2014 that will focus on the advancement of privacy engineering to aid in the development of privacy standards and best practices.

## Venable News

### NHTSA Administrator David L. Strickland Joins DC Regulatory Group

*Top DOT official and former Senate committee counsel, who oversaw increased environmental and safety standards at NHTSA, joins Venable's highly rated group*

Building on the strength of its Regulatory and Legislative practices, Venable LLP announced that David L. Strickland, Administrator of the National Highway Traffic Safety Administration (NHTSA), joined the firm's Washington, DC office as partner in January.

Nominated by President Barack Obama and confirmed by the United States Senate, Mr. Strickland has served as NHTSA Administrator since 2010. Through his position as the country's top automotive safety official, Mr. Strickland has overseen the development of the first national fuel efficiency program in conjunction with the Environmental Protection Agency, issued the first ever ejection mitigation standards for passenger vehicles to help keep passengers from being partially or fully ejected from vehicles during a rollover crash, and brought national attention to child passenger safety issues.

While at NHTSA, Mr. Strickland oversaw a broad range of vehicle safety and policymaking programs including setting vehicle safety standards, investigating possible safety defects, and tracking safety-related recalls; establishing and enforcing regulations on fuel economy; investigating odometer fraud and publishing vehicle theft data. He has also been a leader in the campaign to prevent distracted driving.

Prior to his tenure as the NHTSA Administrator, Mr. Strickland spent eight years on the staff of the U.S. Senate Committee on Commerce, Science and Transportation as Senior Counsel. Through this position he served as lead counsel for subcommittees overseeing the Federal Trade Commission (FTC), the Consumer Product Safety Commission (CPSC), NHTSA, and the Department of Commerce. Mr. Strickland provided legal and legislative advice to Members on a range of issues including insurance, antitrust, consumer protection and fraud prevention, internet privacy, tourism, consumer product safety and liability, passenger motor vehicle safety and fuel efficiency, and the U.S. Olympic Committee.

“An advocate for public safety on the roads, David has impressed the industry with his accomplishments,” said Brock R. Landry, co-chair of Venable’s Government Division. “From the Hill to the Administration, David is well respected and understands the often complex regulatory process from different points of view. He will play a key role in the ongoing growth of our Government Affairs, Automotive, and Technology practices.” Stuart P. Ingis, Partner-in-Charge of the Washington, DC office added, “David is a problem solver and consensus builder, both critical traits to effectively representing clients in Washington. David is a tireless advocate in everything he has done. We are thrilled to have him as part of the Venable team and I know he’ll bring the same passion and energy to our clients that he brought to his public service.”

Commenting on his move to Venable, Mr. Strickland said, “It has been an honor to focus on auto safety for the past four years, however, most of my work in public service has been on broad consumer protection policy, including FTC and CPSC issues. Venable has one of the strongest regulatory and consumer protection policy practices in America. Joining this team of extremely talented attorneys and experts to help develop cross-cutting and thoughtful solutions captures what I envisioned in a full service firm. I could not be more excited to be joining them.”

“With federal regulations impacting our daily lives in more ways than most people can imagine, Venable knows how to navigate through and how to get things done. I’m looking forward to this new challenge and bringing my experience to one of the top teams in the country,” he added.

At Venable, Mr. Strickland joins a bipartisan team of senior Washington insiders including former U.S. Senator Birch Bayh, former U.S. Secretary of Transportation James H. Burnley IV and former Congressman Bart Stupak. The team also includes former veteran Capitol Hill legislative staffers and Executive Branch policy advisors and regulators from both sides of the aisle.

Venable was recently recognized by U.S. News-Best Lawyers "Best Law Firms" as a Tier 1 firm Nationally and in Washington, DC for Litigation - Regulatory Enforcement (SEC, Telecom, Energy) and Tier 1 in Washington, DC for Administrative / Regulatory Law.

Mr. Strickland earned his J.D. from Harvard Law School in 1993 and a B.S. from Northwestern University in 1990.

**********

## About Venable

An *American Lawyer Global 100* law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

Venable's Privacy and Data Security Team serves clients from these office locations:


WASHINGTON, DC
575 SEVENTH STREET NW
WASHINGTON, DC 20004
**t** 202.344.4000
**f** 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
**t** 212.307.5500
**f** 212.307.5598

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
**t** 703.760.1600
**f** 703.821.8949

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
**t** 310.229.9900
**f** 310.229.9901

SAN FRANCISCO, CA
SPEAR TOWER, 40th FLOOR
ONE MARKET PLAZA
1 MARKET STREEET
SAN FRANCISCO, CA 94105
**t** 415.653.3750
**f** 415.653.3755

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
**t** 410.244.7400
**f** 410.244.7742

VENABLE® LLP

## ARTICLES

**January 2014**

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


### AUTHORS

Armand J. (A.J.) Zottola
Robert F. Parr


### RELATED PRACTICES

Technology Transactions and Outsourcing
Labor and Employment

### RELATED INDUSTRIES

Nonprofit Organizations and Associations


### ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007


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

**BYOD Policy**

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

**Expectations of Privacy**

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

**Data Security**

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

**Intellectual Property Protection**

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

**Agency**

BYOD programs may expand an employee's scope of employment by combining the workplace with the private sphere. Under certain circumstances, an employer can even be held liable for the tortious

conduct or criminal behavior of its employees or the binding obligations and contracts they establish with third parties. Clearly define what constitutes work and private use to mitigate exposure to this vicarious liability.

**Employee Disability**

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

**Labor and Employment Issues**

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

**Ongoing Effort**

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

* * * * *

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

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

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

* * * * *

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

VENABLE LLP

technology transactions & outsourcing alert

AUTHORS:

**Armand Zottola**
AJZottola@Venable.com
202.344.8546

**Robert Parr**
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[1] (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).

[1] 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**

VENABLE® LLP

## TECHNOLOGY TRANSACTIONS ALERT

**April 2013**

# INFORMATION SECURITY IMPLICATIONS FOR BUSINESS AGREEMENTS


### AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr


### RELATED PRACTICES

Technology Transactions and Outsourcing

Corporate


### ARCHIVES

2014 2010 2006

2013 2009 2005

2012 2008 2004

2011 2007



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


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**.

VENABLE® LLP

# are you at risk?

## TEN QUESTIONS YOU SHOULD ASK YOURSELF TO ENSURE YOUR CORPORATE PRIVACY HEALTH.

### Q 1. DO I USE INFORMATION ABOUT CUSTOMERS FOR MARKETING OR OTHER PURPOSES NOT RELATED TO THE PARTICULAR SALE OR TRANSACTION IN WHICH I COLLECTED THE INFORMATION?

Using or disclosing information about individuals for a "secondary purpose" – a purpose not directly related to the purpose for which the information was collected – lies at the heart of existing consumer privacy laws, and those that are being debated in legislatures across the country. If you answered yes to this question, your activity may trigger the requirements of existing privacy laws.

### Q 2. DO I COLLECT CONTACT INFORMATION FROM CUSTOMERS WHEN THEY USE THEIR CREDIT CARD TO PAY FOR PURCHASES?

Some states restrict the circumstances under which a seller can use a consumer's telephone number or address (even merely a zip code) if the data was collected from a credit card purchase. If you answered yes to this question, your activity may trigger the requirements of existing privacy laws.

### Q 3. DO I ASK VISITORS TO MY WEB SITE TO TELL ME THEIR AGE? DO I MARKET ANYTHING TO CHILDREN ONLINE?

Online activities affecting children under age 13 are regulated by federal law and standards issued by the National Advertising Council. These laws and standards apply if a Web site or App either "knows" (e.g., knowledge gained by asking for age), or "should have known," that it is interacting with a child. If you answered yes to either of these questions, and collect information that can be linked to a child (e.g., first and last name, email address), your activity triggers the requirements of the Children's Online Privacy Protection Act.

### Q 4. DO I RETAIN CREDIT CARD INFORMATION?

Companies who retain their customers' credit card information are required by law and card brand rules to take certain measures to ensure the protection of that information. If you answered yes to this question, in some circumstances you may be subject to penalties running into the millions of dollars and loss of merchant accounts.

### Q 5. DO I HAVE A PRIVACY POLICY ON MY WEB SITE? IF SO, AM I DOING WHAT I TELL MY CUSTOMERS I AM DOING WITH THEIR PERSONAL INFORMATION?

Most companies voluntarily post privacy policies on their Web sites to help foster trust and confidence; California law requires online merchants to post a privacy policy on their Web sites. Either way, once a company posts a privacy policy on its Web site, federal and state laws against deceptive practices require the company to fulfill the commitments in that policy. If you answered yes to this question, you are subject to the laws prohibiting deceptive practices.

**TO ENSURE YOUR COMPANY'S PRIVACY HEALTH, PLEASE CONTACT US TODAY.**

**EMILIO W. CIVIDANES**
202.344.4414
ecividanes@Venable.com

**STUART P. INGIS**
202.344.4613
singis@Venable.com

### Q 6. DO I CONDUCT BUSINESS WITH COMPANIES IN THE HEALTH CARE, FINANCIAL SERVICES, OR TELECOMMUNICATIONS SECTORS?

Standards mandated by federal and state privacy laws regulating companies within the health care, financial services, and telecommunications sectors extend to vendors and others that provide services to these regulated entities. If you answered yes to this question, you are likely operating under contractual requirements mandated by federal privacy laws.

### Q 7. DO I DO WHAT I TELL MY EMPLOYEES I WILL DO WITH THEIR PERSONAL INFORMATION? DO I TELL MY EMPLOYEES HOW I MONITOR THEM IN THE WORKPLACE?

Employers have access to sensitive information about their employees collected in the ordinary course of business, including data collected as a result of monitoring or evaluating employee performance. Employees typically have very limited privacy rights in the workplace, but their rights can expand if you make commitments to them concerning use of that information. If you answered no to either of these questions, your activity raises privacy issues and may in fact trigger the requirements of existing workplace privacy laws.

### Q 8. DO I RECEIVE PERSONAL INFORMATION (ABOUT CUSTOMERS, EMPLOYEES, VENDORS, OR OTHERS) FROM EUROPE OR OTHER FOREIGN JURISDICTIONS? DO I "OFFSHORE" OR OTHERWISE TRANSFER PERSONAL INFORMATION TO FOREIGN JURISDICTIONS?

Countries in Europe, Asia and Latin America approach privacy differently (some would say more stringently) than we do in the United States. They tend to place restrictions upon the transfer to the United States of information about individuals, even if the information does not pertain to consumers or employees, and even if the parties transferring the information are corporate affiliates. Conversely, U.S. laws often mandate that companies transferring personal information to vendors or subcontractors in foreign countries must require these data recipients to comply with U.S. privacy or security standards. If you answered yes to either of these questions, your activity may be subject to foreign data protection laws or U.S. privacy laws.

### Q 9. DO I HAVE AN EFFECTIVE SECURITY PROGRAM DESIGNED TO SAFEGUARD PERSONAL INFORMATION?

Without security protections for personal information, there is no privacy. As a result, federal and state laws mandate that companies develop, implement, and periodically update programs designed to protect its confidentiality. These security obligations often exceed the safeguards that you would implement to protect your proprietary interests in the data. If you answered no to this question, you could be found in violation of law, even if the persons whose information you are storing have suffered no harm.

### Q 10. DO I HAVE AN EFFECTIVE MITIGATION PLAN FOR PRIVACY OR SECURITY BREACHES?

Breaches of security that compromise personal information are virtually inevitable. Businesses not only must have procedures in place to prevent security breaches, but also procedures in place to respond to such breaches when they occur. Nearly all 50 states have laws requiring notification of affected individuals when their personal information has been compromised by a security breach. If you answered no to this question, you are likely to make hasty decisions when you discover a suspected security breach, which increases the chances you will violate the breach notification laws.

VENABLE® LLP

1.888.VENABLE
www.Venable.com