March 2015

# the download

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

## VENABLE SNAPSHOT

Received *Chambers USA* "Award of Excellence" for the top privacy practice in the United States

Named Two of the "Top 25 Privacy Experts" by *Computerworld*

"Winning particular plaudits" for "sophisticated enforcement work" – *Chambers and Partners*

Recognized by *Chambers Global* and the *Legal 500* as a top law firm for its outstanding data protection and privacy practice


## ISSUE EDITORS:

Stuart P. Ingis
singis@Venable.com

Michael A. Signorelli
masignorelli@Venable.com

Ariel S. Wolf
awolf@Venable.com

## ADDITIONAL CONTRIBUTORS:

Emilio W. Cividanes
ecividanes@Venable.com

David L. Strickland
dlstrickland@Venable.com

Julia Kernochan Tama
jktama@Venable.com

Kelly A. DeMarchis
kademarchis@Venable.com

Tara Sugiyama Potashnik
tspotashnik@Venable.com

Matt H. MacKenzie
mhmackenzie@Venable.com

Rob L. Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

Marissa L. Kibler


## Introduction

In the March issue of *The Download*, we review a number of privacy and data security developments across the gamut of legal and policy channels. Congressional interest and activity in data security picked up in pace and scope with committees on both sides of Capitol Hill holding hearings. The White House convened its awaited "Cybersecurity Summit" and the President announced new executive orders and initiatives. Yet developments were not confined to the federal government. State lawmakers proposed new data security laws in the wake of public data breaches, while several international bodies continued activities related to privacy regulation. In the marketplace, we report on a rollout of a mobile and app choice tool announced by the Digital Advertising Alliance.

## In this Issue:

## Heard on the Hill

### Senate Commerce Committee Holds Hearing on Internet of Things

On February 11, the Senate Committee on Commerce, Science, and Transportation held a hearing entitled "The Connected World: Examining the Internet of Things." The hearing focused on the growing use of smart devices in the daily lives of consumers, from smart thermostats to fitness trackers. The hearing, which featured testimony from several industry representatives as well as from academic experts, explored benefits and challenges that the Internet of Things ("IoT") presents to consumers and businesses. The hearing was requested in October, 2014, by a bipartisan group of senators serving on the Commerce Committee who have pledged to examine the issues surrounding the IoT in the 114th Congress.

In their opening statements, Chairman John Thune (R-SD) and Ranking Member Bill Nelson (D-FL) shaped the discussion around the benefits and challenges of the IoT. Chairman Thune cautioned the Committee to "tread carefully and thoughtfully" before imposing government intervention that "could halt innovation and growth," and called for treating the IoT with "the same light touch that has caused the Internet to be such a great American success story."[1] Ranking Member Bill Nelson (D-FL) labeled the threat of overregulation a "red herring" and stated that the "promise of the Internet of Things must be balanced with real concerns of privacy and the security of our networks."[2]

Members and panelists at the hearing discussed issues of data security, consumer choice, and interoperability, as well as data ownership and transfer. Some participants raised concerns about the ability of bad actors to hijack consumer devices, especially cars and medical devices, and inflict harm on consumers in some way. At the same time, participants recognized that the IoT is in a nascent stage and that as it continues to develop it will provide consumers with value. From a policy perspective, participants discussed the role of government in regulating the IoT space, focusing on the activity of the Federal Trade Commission in enforcing data security standards, and the availability of spectrum for IoT development. Senator Ed Markey (D-MA) announced plans to introduce legislation intended to address privacy and security risks of connected automobiles, which follows the release of a report he authored on the same topic.

Members of the House of Representative have also expressed interest in IoT issues. On January 13, Representatives Darrel Issa (R-CA) and Suzan DelBene (D-WA) announced the launch of the new Congressional Caucus on the Internet of Things. The Caucus will focus on the issues facing the growing IoT marketplace, including data collection and sharing. The Caucus will educate members about the IoT sector and how IoT devices present opportunities and challenges for businesses and consumers.

### Congress Holds Hearing on Student Privacy

On February 12, 2015, the U.S. House Education and the Workforce Committee's Subcommittee on Early Childhood, Elementary, and Secondary Education ("Subcommittee") held a hearing entitled "How Emerging Technology Affects Student Privacy." Witnesses included representatives from industry, academia, the public school system, and an advocacy group. The hearing focused on whether legislation should be introduced to modify the Family Educational Rights and Privacy Act ("FERPA"). Participants also weighed in on potential privacy and security issues that may arise from emerging technologies that bolster student data.

Subcommittee Chairman Todd Rokita (R-IN), Subcommittee Ranking Member Marcia Fudge (D-OH), and other members of the Subcommittee stated their support for legislation to update FERPA to address new technologies. California's Student Online Personal Information Privacy Act (SOPIPA) was cited by some Subcommittee members as an appropriate model for drafting such legislation. There was general agreement among hearing participants that the legislation should prohibit the use of student data for marketing purposes, including for targeted advertising and profiling. Other considerations that were discussed included requiring parties that collect and use student data to adopt certain security measures, extending protections for certain types of student data not addressed under existing federal law (*e.g.*, metadata), providing redress options for students and parents, and broadening enforcement authority.

The representative from the public school system cautioned lawmakers against drafting legislation that would impede certain measures that schools may have in place to protect student information, noting that the school district she represents

[1] *The Connected World: Examining the Internet of Things: Hearing before the S. Comm. on Commerce, Science, and Transportation*, 114th Cong. (2015) (statement of Chairman John Thune).

[2] *Id* (statement of Ranking Member Bill Nelson).

emphasizes anonymization of student data and ensures that vendor contracts specify limits on the use of such data. The witness representing academia interests stated that anonymized student data may be reverse-engineered to become identifiable. With regard to a recent industry effort where certain companies and organizations publicly commit to prohibit certain activities that may harm student privacy, such as selling student information, Rep. Suzanne Bonamici (D-OR) raised her concern regarding enforcement, noting that the Federal Trade Commission (FTC) could not use its Section 5 deceptive and unfair practices authority to represent individuals in cases where a violation by a member is not widespread.

On a related note, Reps. Jared Polis (D-CO) and Luke Messer (R-IN) have recently announced that they will introduce bipartisan student data privacy legislation, which they have been working on with the White House. The White House has not yet released its final legislative proposal modeled after California's SOPIPA, which the President announced in January during a speech at the FTC. Senator Edward Markey (D-MA), who introduced the "Protecting Student Privacy Act of 2014" (S.2690) last year, has recently stated that he plans on introducing student privacy legislation this term.

### Senator Markey Issues Report on Privacy and Security of Vehicles

On February 9, 2015, Senator Edward J. Markey (D-Mass.) released a report entitled "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk."[3] The report compiles the responses of sixteen major automobile manufacturers to a series of questions that Sen. Markey posed to each manufacturer in a letter sent on December 2, 2013. The report made eight key findings, including that: (1) nearly all cars on the market include wireless technologies; (2) most automobile manufacturers were unaware of or unable to report on past hacking incidents; (3) security measures to prevent remote access to vehicle electronics are inconsistent across manufacturers; (4) most manufacturers are not capable of diagnosing or responding to an infiltration in real time; (5) manufacturers collect large amounts of data on driving history and vehicle performance; (6) most manufacturers offer technologies that collect and wirelessly transmit driving history data to data centers without effectively securing the data; (7) manufacturers' practices with respect to the use and storage of personal vehicle data varies considerably; and (8) customers are often not made aware of data collection, or they cannot opt out without disabling certain features.

The report highlighted two primary areas of concern: security measures to prevent hackers from gaining control over vehicle components and the collection and use of location or driving history data. The report also called on the National Highway Traffic Safety Administration, with the assistance of the Federal Trade Commission on privacy issues, to promulgate new standards to protect the data, security, and privacy of drivers. The report further suggested that such standards should address the following issues: (1) ensuring that vehicles with wireless access points and data-collecting features are protected against hacking and security breaches; (2) validating security features through the use of penetration testing; (3) including measures to allow manufacturers to respond in real time to hacking events; (4) requiring that drivers are made explicitly aware of the collection, transmission, and use of driver data; (5) providing drivers with an opportunity to opt out of the collection and transfer of driver data; and (6) allowing consumers to request that personally identifiable information be removed prior to transmission when possible.

The auto industry has been proactive in these areas, particularly on interconnected cars. For example, last November the Association of Global Automakers and the Alliance for Automobile Manufacturers unveiled auto industry consumer privacy protection principles based on the Federal Trade Commission's Fair Information Practice Principles. The automakers' privacy principles are part of a larger initiative by automakers to protect the privacy and security of the data necessary to support advanced vehicle technologies. Despite the absence of reported hacking incidents affecting vehicles on the road to date, as noted in the Markey report, the industry also has announced measures to prepare for threats by working to establish a mechanism for sharing vehicle cybersecurity information among the auto sector.

---

## From the White House

### White House Convenes Summit on Cybersecurity

On February 13, the White House convened a "Summit on Cybersecurity and Consumer Protection," which was hosted at Stanford University. Speakers and panelists at the summit discussed a range of topics related to cybersecurity, but one common theme that arose was public-private collaboration on cybersecurity, for which the President advocated in his remarks. During the panel devoted to this subject, participants, CEOs representing industries ranging from financial services to health care, as well as U.S.

[3] See http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

Secretary of Homeland Security Jeh Johnson and U.S. Deputy Secretary of Energy Dr. Elizabeth Sherwood-Randall, noted a dearth of information that is currently available on cybersecurity threats, despite collaborative efforts already in place. Another panel, which included U.S. Secretary of Commerce Penny Pritzker and CEOs from the financial services and consumer protection industries, assessed the value and effectiveness of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, and participants highlighted the need for flexible standards to meet constantly evolving threats. U.S. Deputy Secretary of Treasury Sarah Bloom Raskin moderated a panel of CEOs from the financial services and retail sectors, during which panelists focused on authentication and consumer trust with respect to payment technologies.

While Secretary Johnson, Secretary Pritzker, and Homeland Security Advisor Lisa Monaco pushed for legislation enabling cybersecurity information sharing, others, representing payments and technology companies, encouraged other measures such as security-by-design and new forms of authentication. Industry representatives discussed the importance of training employees at all levels of an organization to be aware of security concerns and appropriate responses, in addition to a company's reliance on security experts. Generally, industry representatives underscored the importance to the economy of the Internet and its architecture and infrastructure.

At the summit, President Obama announced the launch of a new "Cyber Threat Intelligence Integration Center," which will identify and analyze cyber threats across federal agencies. The President also announced the issuance of an executive order titled "Promoting Private Sector Cybersecurity Information Sharing," which encourages voluntary cybersecurity risk information sharing across the public and private sectors.

### President Obama Signs Executive Order on Information Sharing and Cybersecurity

On February 13, 2015, the President signed an Executive Order to promote private sector cybersecurity information sharing. The purpose of the Order is to encourage the voluntary formation of Information Sharing and Analysis Organizations (ISAOs) and to allow these organizations to partner with the federal government on a voluntary basis. The order directs the Secretary of Homeland Security ("Secretary") to encourage the development and formation of ISAOs by selecting a nongovernmental organization that will be responsible for identifying a common set of voluntary standards for the creation and functioning of ISAOs. The standards must address the baseline capabilities that ISAOs should possess, as well as the contractual agreements, business processes, operating procedures, technical means, and privacy protections for ISAO operation. The standards must also be consistent with voluntary international standards when such standards will advance the purpose of the Order and must meet the requirements of the National Technology Transfer and Advancement Act.

The Order further designated the National Cybersecurity and Communications Integration Center (NCCIC) as a critical infrastructure protection program and authorized it to enter into agreements with ISAOs to promote critical infrastructure cybersecurity. It directed the NCCIC to coordinate with ISAOs to promote the sharing of information pertaining to cybersecurity risks and incidents, and it directed the NCCIC and other federal agencies involved in sharing cybersecurity threat and incident information to ensure that such information sharing incorporates the appropriate privacy protection principles, which should be based on the Fair Information Practice Principles and other privacy and civil liberties policies as appropriate.

---

## Around the Agencies

### FAA Proposes Regulations for Small Commercial Drone Use

The Federal Aviation Administration ("FAA") recently proposed new regulations to govern commercial and government use of small drones weighing up to 55 pounds, although it may take years to finalize a regulatory framework. The agency is likely to put forward separate rules for larger drones as well as for "micro drones" weighing up to 4.4 pounds.

The proposed regulations would set forth specific rules for commercial drone use, but contain numerous restrictions. For example, businesses would be limited to flying drones during daylight hours, under 100 miles per hour and 500 feet of altitude, and within eyesight of the operator or other observers. These proposed rules could limit the use of drones for long-distance deliveries unless the regulations are modified.

However, the FAA has proposed that there would be no requirement to obtain a pilot's license or pass a flying test to operate this type of drone. Rather, operators would need to take a written exam and register the drone. This approach could place

drone use within reach of smaller businesses.

In a related development, President Obama issued an executive order that articulates a policy framework, including greater transparency, for the federal government's use of drones. Under this order, federal agencies will need to disclose where they use drones within the United States, and how they store and protect personal information from such flights. Agencies also must publish annual reports on drone use over the preceding year.

President Obama also tasked the Commerce Department with convening a multi-stakeholder process, within 90 days, to develop a voluntary code of conduct on privacy, transparency, and accountability issues related to commercial and other private drone use. This process would follow the model the Commerce Department has used to promote other such codes on privacy issues, which are intended to implement the White House's 2012 consumer privacy framework.

---

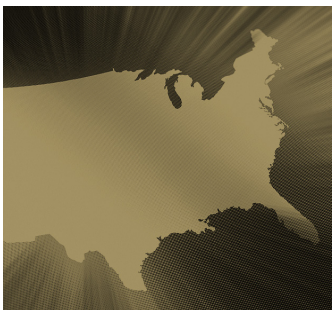
## In the Marketplace

### DAA Launches AppChoices and Mobile Web Tool

In late February, the Digital Advertising Alliance ("DAA") released two new mobile consumer choice tools, AppChoices and a DAA Consumer Choice Page for Mobile Web. These new tools allow consumers to exercise choice over the collection and use of data from mobile devices for online behavioral advertising. In the summer of 2013, DAA issued guidance concerning the application of the DAA Principles to the mobile environment.

These new tools build on the success of the DAA Choice Page, which gives consumers control of the collection, transfer, and use of web viewing data for online behavioral advertising on their desktop browsers. The app and mobile site allow consumers to make granular choices about which companies participating in the tools may collect and use data from their device in order to deliver relevant advertising to them. The AppChoices launched with eighteen participating companies, with plans of expansion throughout the year. AppChoices is available for free on the Apple, Amazon, and Google application stores, and the Mobile Choice Page is available through your device browser at www.aboutads.info.

---



## In the States

### CT State Senate Proposes Bill that Would Require Health Insurers to Encrypt Customer Information

Following a publicly reported data breach of a health care company on January 29, 2015, Democratic Party leaders in the Connecticut state senate have announced plans to introduce legislation that would require health insurance companies operating in Connecticut to encrypt all personal information records stored and transmitted by the companies. The proposal also calls for health insurance companies that store or transmit personal information to limit future risks by adopting secure user authentication protocols (such as mandatory user IDs, unique passwords, etc.) and upgrading information safeguards. Other details of the legislation, including how it would be enforced, have yet to be released.

State Senate Majority Leader Bob Duff stated that the effort in Connecticut was intended to limit what information hackers could acquire and to render any such information useless. He cited cybersecurity experts who noted that encryption technology would limit the amount of data that any user, even an authorized one, could view at any one time. Other experts have questioned whether the proposed encryption law would have stopped the breach that has prompted the legislative activity in Connecticut.

The proposal follows a similar legislative effort in the State of New Jersey to require health insurance carriers to encrypt personal information. Several other states have enacted data security standards of general applicability, including standards that call for encryption where reasonable. The Health Insurance Portability and Accountability Act (HIPAA) calls for health insurers and other "covered entities" to encrypt stored or transmitted health information, where "reasonable and appropriate." During the press conference announcing the proposal, State Senator Martin Looney noted that legislators view

the lack of an encryption mandate in HIPAA as a gap in federal law that requires action at the state level.

### NJ State Senate Repeals Zip Code requirement on gift card purchases

On February 5, 2015, New Jersey Governor Chris Christie signed into law NJ S 2235/AB 3480, a law that repeals the requirement on retailers to collect zip code information from the purchasers of Stored Value Cards (SVCs), or gift cards. This development follows from a state law enacted in 2010 that allowed the state to claim unused gift card balances after two years. The 2010 law included a provision that required gift card retailers to record, at a minimum, a gift card customer's zip code as a means of aiding the state in establishing the residency of the card's holder and validating the State's claim on unused gift card value.

The 2010 law met significant opposition from the SVC industry and related businesses, leading to the passage in 2012 of a compromise measure that modified a number of provisions in the original law. However, the zip code collection requirement was not repealed until passage of the February 2015 measure.

New Jersey originally enacted the zip code collection requirement in order to buttress its claim on the escheat of unused gift card balances. After the U.S. Court of Appeals for the Third Circuit ruled that the physical purchase of a gift card within a state was not sufficient to establish that state's escheat of the unused value of that card after the abandonment period,[4] New Jersey added the zip code collection requirement in order to establish the residency of the card holder and shore up its claim on any unused value. Although the state estimates that it will lose $17.5 million in escheat collections by 2023,[5] the repeal of the zip code collection requirement eases a recording burden for retailers and providers of SVCs and will prevent the exit of some of the nation's largest SVC providers from the New Jersey gift card market. The new law leaves in place the rest of the provisions of the 2012 "compromise," including a 5 year abandonment period, the elimination of expiration dates for SVCs, and a split of the claim on unused gift card balances with 60% going to the state and 40% going to the SVC issuer.

---


## International

### Article 29 Working Party Releases Opinion on Health Data and Mobile Apps

On February 5, the European Union Article 29 Working Party published a letter clarifying the scope of "health" data relative to lifestyle and wellbeing mobile apps. The Article 29 Working Party is comprised of representatives of different EU governing bodies and is tasked with providing advice to the European Commission ("EC") on data protection.

Under the EU Data Protection Directive (95/46/EC), personal data related to health is subject to a heightened level of protection. Specifically, collecting health information, which is considered "sensitive," generally requires explicit or, "unambiguous" consent. Other EU data protection principles, such as transparency, purpose limitation (limiting the processing of data for purposes other than those disclosed at collection), and security also apply. At present, the Directive does not, however, define what type of information is regarded as health data. With the proliferation of lifestyle, exercise, and related health apps, the EC sought clarification on the definition of health data in this ecosystem.

As a threshold matter, the opinion acknowledges that medical data, defined as data about the physical or mental health status of an individual that is generated in a professional, medical context, is clearly health data. This would include all data related to diagnosis and/or treatment by health services professionals and related information on diseases, disabilities, medical history and clinical treatment. Any of this data when captured by a mobile device or app would be included, even if the mobile device is not a "medical device."

Aside from this conventional definition, the letter briefly cites the broad range of data types that have been found to be health related, including the fact that someone has broken her leg or wears glasses or contact lenses, IQ, smoking and drinking habits, allergies, information that a child attended summer camp for asthma sufferers, membership in Weight Watchers, and mentioning that someone is ill in an employment context.

Based on the potential breadth of the definition of health information, the Working Party recognized two other categories

[4] N.J. Retail Merchants Ass'n v. Sidamon-Eristoff, 669 F.3d 374 (3d Cir. 2012).

[5] Office of the State Treasurer, State of New Jersey, Treasury Announcement FY 2011-03, Guidance on Implementation and Notice of Exemption from Certain Provisions of L.2010, c.25, at 3 (Sept. 23, 2010).

of health information. First, health information includes data used in an administrative context, such as data disclosed to public bodies on whether one's household includes individuals with specific diseases and/or disabilities for the purpose of tax deductions or similar allowances. In addition, health data also includes data about the purchase of medical products, devices and services, when health status can be inferred from the data, or information about the participation in some selectively performed screening tests, such as tests for rare diseases.

On the other hand, the Working Party assumes that some data generated by these apps is not to be regarded as health data. This data would include information from which no conclusions can reasonably be drawn about the user's health status, which it calls "raw personal data." It gives as the example pedometer apps that count steps, where, provided the data cannot be combined with other data about the user and is not framed by a medical context, nothing about the user's health can be inferred. However, the same data, aggregated over time in combination with age and sex, could become health data as it can be used to determine a significant aspect of the person's health, such as risk for obesity.

### UK ICO Rolls Out Privacy Seals Proposal

On January 28, the UK Information Commissioner's Office (ICO) published details of plans to have a privacy seal program "up and running" in 2016.[6] Under this plan, businesses will be able to apply to privacy seal scheme operators, which would endorse businesses with the use of a symbol to signify that the company is "going above and beyond the call of duty" with respect to security of personal information. Specifically, operators would look to see whether the applicant is doing more than what is required by the Data Protection Act.

First, the ICO will identify and authorize operators of the schemes in a variety of fields, such as mobile apps and health information. This approach will allow businesses that want to apply for privacy seals to work with operators who are already familiar with the privacy concerns and practices in those areas. Once those operators have been selected, they will be announced so that companies can apply to the operators for an ICO privacy seal.

The ICO stated that the new program will give endorsed companies a competitive advantage, help build consumer trust and choice, and raise privacy standards across the UK. However, the ICO has noted that the Office may take away a company's privacy seal endorsement if the company does not maintain the required high standards. For instance, a "serious breach" could cause a company to lose its seal.

---

## About Venable's Privacy and Data Security Team

Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed in the evolving U.S., Canadian, European and Asian regulations governing our clients' businesses, and assist with drafting statutes and regulations. Our clients represent a variety of industries and are supported by Venable's renowned Legislative and Government Affairs, Advertising, IP and Communications Practices. Venable's Privacy and Data Security Practice is recognized in Chambers Global and the U.S. Legal 500 and has won the Chambers USA Award for Excellence.

## 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
t 202.344.4000

NEW YORK, NY
t 212.307.5500

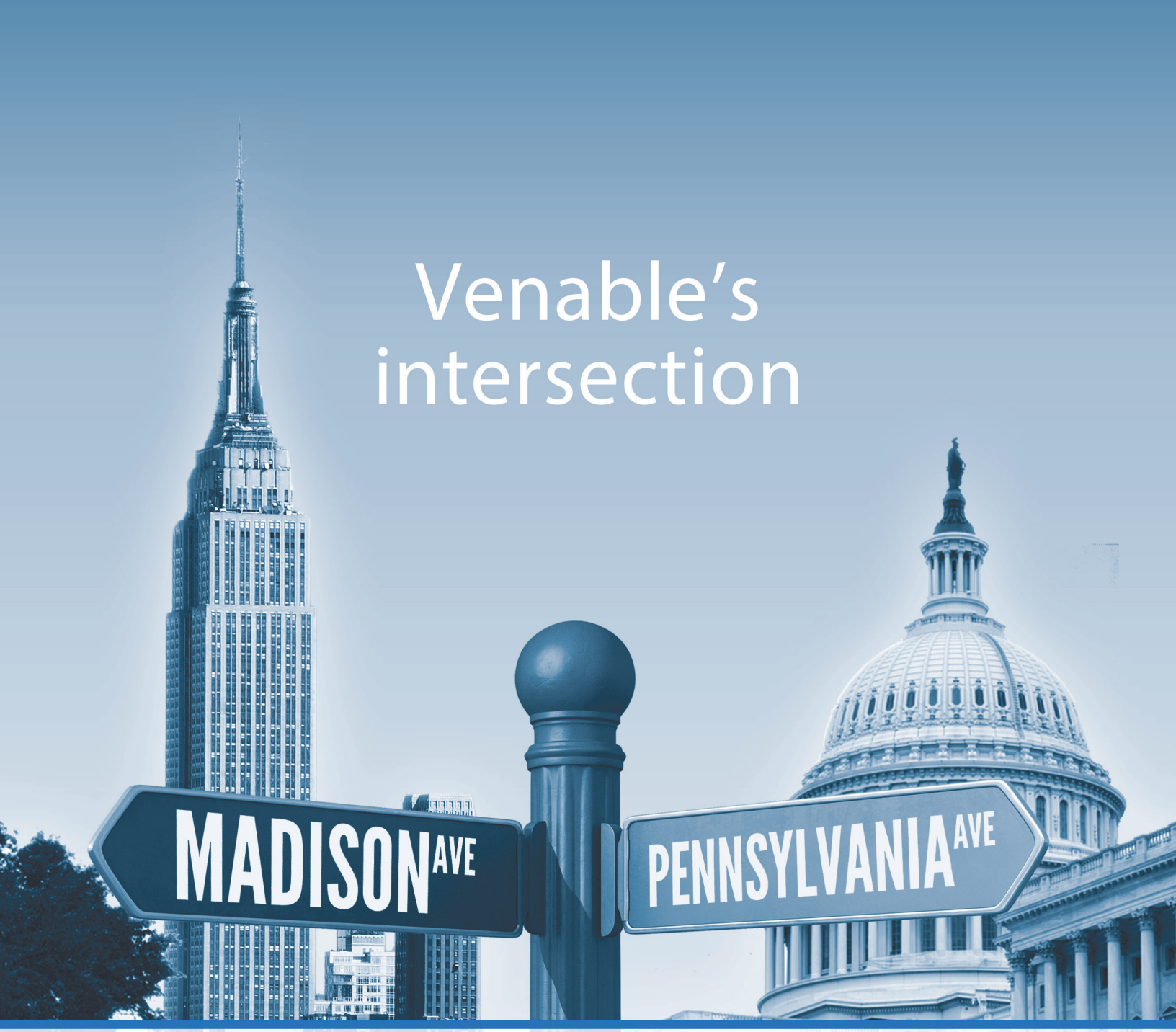
SAN FRANCISCO, CA
t 415.653.3750

LOS ANGELES, CA
t 310.229.9900

BALTIMORE, MD
t 410.244.7400

TYSONS CORNER, VA
t 703.760.1600

[6] Gemma Farmer, What You Need to Know About ICO Privacy Seals, Information Commissioner's Office (Jan. 28, 2015), *available* at https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/.




## The law firm advertisers turn to for regulatory, policy and enforcement issues.