September 2015

the download

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

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 Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

POLICY ANALYSTS:

Marissa Kibler

London Swift

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

Introduction:

In this issue, we cover developments in both chambers of Congress where Members engaged in privacy and data security issues, including those related to the Internet of Things, with the House Judiciary Committee holding a hearing on the subject and Members of the Senate Commerce Committee introducing legislation on auto privacy and security. We recap regulatory and policy efforts by the federal agencies including the FTC's requested guidance on an update to COPPA, and the GAO's report on facial recognition technology, among other developments in the Executive Branch. Several states took steps to update their data security and breach notification laws, and a U.S. Court of Appeals issued a decision likely to have an impact on data breach class actions in the future. Finally, we review guidance issued by a Russian government ministry to clarify the country's new data localization law that took effect September 1.

In this Issue:

Heard on the Hill

Senators Introduce Auto Privacy and Security Bill

On July 21, 2015, Senators Ed Markey (D-MA) and Richard Blumenthal (D-CT) introduced the Security and Privacy in Your Car Act of 2015. The stated purpose of the "SPY" Act, or S.1806, is to protect consumers from security and privacy threats to their motor vehicles. The bill would require the establishment of federal standards governing the privacy and security of electronic systems connected to motor vehicles and the data stored onboard the vehicle, in transit from the vehicle to another location, and in any subsequent off board storage or use. The bill would set penalties for violating these standards at a maximum of $5,000 per violation.

The SPY Act would require the National Highway Transportation Safety Administration ("NHTSA"), in consultation with the Federal Trade Commission ("FTC"), to issue regulations to prevent hacking into vehicle control systems. The standards would require that all access points be equipped with reasonable measures to protect against hacking attacks, including the isolation of critical software systems. The standards would further require that vehicle security be evaluated using best security practices. The bill would also require that data collected by the vehicle be secured to prevent unauthorized access, and that the vehicle be capable of detecting, reporting, and stopping real-time hacking attempts. These standards would be reviewed every three years to ensure that they are adequate.

On the data privacy front, the bill would require the FTC to develop privacy standards for the data collected by the vehicle. These standards would require that vehicle owners are made explicitly aware of the collection, transmission, retention, and use of driving data. The bill would allow owners to opt out of data collection without losing access to key navigation or other features, except for in the case of electronic data recorders or other safety or regulatory systems. Finally, the bill would prohibit a vehicle manufacturer from using any information collected for marketing or advertising purposes without affirmative express consent by the vehicle owner. A violation of these standards would be considered an unfair and deceptive practice under the FTC Act.

Finally, in an effort to educate the consumer, the bill would require NHTSA to establish a "cyber dashboard" that displays an evaluation of how well each automobile protects both the security and privacy of vehicle owners beyond the minimum standards. Modeled after the agency's 5-Star safety rating program, this information should be presented in a transparent, consumer-friendly form on the window sticker of all new vehicles.

The bill was referred to the Senate Committee on Commerce, Science, and Transportation and, although the committee has not held a legislative hearing or marked up the bill, Senator Markey attempted to include it as an amendment to the Cybersecurity Information Sharing Act (CISA) of 2015, which the Senate considered at the end of July. Ultimately, the Senate was not able to finalize CISA before departing for the August recess, but members did agree on a list of amendments to consider when they return. The SPY Car Act was not included in the resulting list of amendments, so the prospects for its passage remains unclear. While there is no House companion bill, the House Committee on Energy and Commerce Chairman Fred Upton (R-MI) has expressed interest in this issue. Earlier this spring, he wrote to seventeen auto manufacturers to request information about their plans to address vehicle cybersecurity challenges.[1]

The auto industry moved last year to establish an Auto Information Sharing and Analysis Center, which is designed to allow manufacturers to share threat information and best practices to better safeguard the automobile.[2]

House Judiciary Committee Hearing on the Internet of Things

On July 29, 2015, the House Judiciary Committee's ("Committee") Subcommittee on Courts, Intellectual Property, and the Internet ("Subcommittee") held a hearing on the Internet of Things ("IoT"). Subcommittee members and witnesses discussed law enforcement access to private online information, vehicle-to-vehicle communication, spectrum use and allocation, and consumer consent.

Subcommittee Chairman Darrell Issa (R-CA) announced the Committee's plan to explore potential challenges and opportunities associated with connected devices alongside other committees and the Congressional Internet of Things Caucus. Committee Chairman Bob Goodlatte (R-VA) cited examples of the communal benefits of IoT, and stated that the Committee will continue to monitor privacy and data security measures adopted by the industry as the field develops.

Witnesses at the hearing advocated for a national strategy on IoT and highlighted spectrum and high-skilled immigration visa reform as areas Congress should address to foster IoT innovation.

[1] http://energycommerce.house.gov/press-release/committee-leaders-seek-information-auto-cybersecurity.

[2] http://www.autonews.com/article/20141021/OEM11/141029957/auto-industry-forming-consortium-to-fight-hackers.

Around the Agencies

NIST Releases Guidance on Securing Electronic Health Records on Mobile Devices

The National Cybersecurity Center of Excellence ("NCCoE"), a division within the National Institute of Standards and Technology ("NIST"), recently issued an implementation guide to develop a model security design for protecting electronic health records on mobile devices. The implementation guide provides set-up procedures for a number of security arrangements, including Domain Name System ("DNS") servers, access points with IP and MAC address filtering, certificate based access control, and online back-up systems. The guide also contains instructions for implementing an intrusion detection system and a certificate authority system, mobile device network communications, a mobile device management tool, and a governance, risk, and compliance platform.

An assessment of the model design by a third party identified several threats to the security of electronic health records on mobile devices, including: (1) a lost or stolen mobile device, (2) a user who walks away from a logged-on mobile device, downloads viruses or other malware, or uses an unsecure Wi-Fi network, and (3) inadequate access control and/or enforcement; inadequate change management; inadequate configuration management; or inadequate data retention, backup, and recovery.

The guide is not intended as a one size fits all solution, and NCCoE states that organizations can choose to implement all or part of the model design or use it as a starting point for the development of a custom security design.

FTC Seeks Public Comment on Proposal for Parental Verification Method Under COPPA Rule

The FTC is considering a proposal for a new method of obtaining parental consent under the Children's Online Privacy Protection Act ("COPPA").[3] COPPA requires websites and online services that are directed to children under 13, or have actual knowledge that they are collecting information from child users, to provide certain privacy notices and obtain "verifiable parental consent" prior to collecting, using, or disclosing personal information from child users. Under revised COPPA regulations that became effective in 2013, the FTC enumerated certain methods that can be used to acquire parental consent under COPPA, and also established a voluntary process for companies to submit new parental consent methods to the FTC for approval. The FTC has 120 days to respond to such proposals.

Jest8 Limited, trading as Riyo ("Riyo"), has proposed that companies should be able to obtain parental consent under COPPA by matching a parent's facial image with a verified photo identification.[4] This process has been implemented in other authentication scenarios. According to Riyo's proposal, the proposed system first verifies the authenticity of a photo identification that is scanned via webcam or device camera. The parent is also asked to take and submit a photographic self-portrait, which is then compared to the facial image from the photo identification document. The Riyo proposal states that no other databases are referenced in this process, and that the identification and image data is stored only for five minutes. Riyo argues that the proposed method provides assurance that the person completing the consent mechanism is the parent.

While comments may address any aspect of the proposal, the FTC requested comment specifically on three questions raised by Riyo's proposal: (1) whether Riyo's proposed method is already covered by the existing methods enumerated in COPPA regulations; (2) whether the proposed method meets COPPA requirements for verifiable parental consent; and (3) whether the proposed method poses a risk to consumers' personal information and, if so, if this risk is outweighed by the method's benefits.[5]

GAO Releases Report on Facial Recognition Technology

On July 30, 2015, the Government Accountability Office ("GAO") released a report entitled "Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law" ("Report").[6] GAO issued the Report in response to a request made last year by Senator Al Franken (D-MN), Ranking Member of the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law, which called on the agency to review the potential privacy implications raised by the commercial use of facial recognition technology ("FRT").

[3] 80 Fed. Reg. 47429 (Aug. 7, 2015).

[4] Letter from Riyo to Donald S. Clark, FTC Secretary (June 30, 2015).

[5] 80 Fed. Reg. 47429 (Aug. 7, 2015).

[6] Government Accountability Office, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law (July 31, 2015), *available at* http://www.gao.gov/assets/680/671764.pdf.

The Report concluded that no federal privacy law specifically addresses the commercial use of FRT, and that certain existing laws that apply to the collection, use, and storage of personal information (e.g., Gramm-Leach-Bliley Act) may pertain to the technology in some contexts. The Report noted that the Federal Trade Commission ("FTC") may have limited enforcement authority over FRT if uses of the technology cause substantial injury to consumers or violate a privacy policy. The Report recommended that Congress enact a federal privacy law to account for emerging technologies and to strengthen the existing privacy legal framework.

The Report noted that the National Telecommunications and Information Administration ("NTIA") Multistakeholder Process on developing a code of conduct for FRT is a step forward to account for privacy considerations in the use and development of the technology. Prior to the Report's release, the NTIA convened its twelfth FRT multistakeholder meeting, where industry representatives and the FTC weighed in on discussion drafts proposed by trade groups that set forth recommendations for a best practices document on the commercial use of FRT. The next NTIA FRT multistakeholder meeting will focus on the proposed discussion drafts and is expected to take place sometime in mid-October.

HIPAA Security Rule Settlement Based on Use of Cloud Provider

Earlier this summer, the U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights announced a settlement with St. Elizabeth's Medical Center in Brighton, Massachusetts for alleged violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Breach Notification Rules. This settlement serves as a reminder to HIPAA covered entities seeking to adopt new software or technology that they cannot do so outside of the HIPAA risk assessment framework.

The settlement arose from a complaint that HHS received from St. Elizabeth's employees in 2012 alleging that St. Elizabeth's was not compliant with HIPAA because it had been using an internet-based document sharing application to store documents containing electronic protected health information ("ePHI"). St. Elizabeth's later notified HHS in 2014 that it had suffered a breach of unsecured ePHI impacting approximately 1,000 individuals.

HIPAA's Security Rule[7] requires entities subject to HIPAA to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. The Security Rule permits covered entities to implement security standards that take into account the size, complexity, and capabilities of the covered entity, their technical infrastructure, probable risks, and cost. Nevertheless, to implement this flexible approach, covered entities are required to conduct an accurate and thorough risk analysis to assess potential risks and vulnerabilities to ePHI. The complaint against St. Elizabeth's was not based on its use of a cloud-based document management system, but on the fact that the risks of implementing such a system had not been assessed. In fact, the 2014 breach was not linked to use of the document shared application but was tied to ePHI on a former employee's personal laptop and on a USB flash drive.

As a condition of settlement, St. Elizabeth's has agreed to pay a resolution amount of $218,400 and implement a Corrective Action Plan. The Corrective Action Plan requires St. Elizabeth's to conduct a self-assessment with a number of specific requirements such as random interviews with employees and random inspections of portable devices. The Corrective Action Plan further obligates St. Elizabeth's to report all violations of HIPAA policies and procedures to HHS, even if the violations do not rise to the level of regulatory violations.

Federal Court

7th Circuit Court of Appeals Grants Article III Standing to Neiman Marcus Data Breach Plaintiff

On July 20, 2015, the Court of Appeals for the Seventh Circuit found that a suit against Neiman Marcus, stemming from its 2013 data breach, satisfied Article III standing requirements.[8] This decision reversed and remanded a district court's decision to the contrary.

In this case, plaintiffs alleged that they suffered several injuries, including lost time and money from fraudulent charges and protecting against identity theft, financial losses from purchases they would not have made if they knew the store would be breached, and lost control of their personal information. Additionally, plaintiffs alleged that future harms were yet to occur and that fraudulent charges were reasonably likely to appear on their credit cards. The Seventh Circuit examined each claim for sufficiency under Article III.

[7] The Security Rule is found at 45 C.F.R. Part 160 and Subparts A and C of Part 164.

[8] *Remijas et. al., v. Neiman Marcus Group*, Decision, No 14-3122 (7th Cir., 2015) *available at* http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2015/D07-20/C:14-3122:J:Wood:aut:T:fnOp:N:1590360:S:0.

The Court made clear that speculative mitigation expenses by consumers do not meet Article III standing. However, the Court also found that the cost of mitigating potential credit card fraud was not speculative because Neiman Marcus offered one year of free credit monitoring to impacted consumers. Because plaintiffs properly alleged that the cost of monitoring was not de minimis, the court found that the alleged injuries of resolving fraudulent charges and protecting from future identity theft met Article III standing requirements. However, the court emphasized that, while it needs to decide the sufficiency of the other allegations, those allegations are more attenuated. Specifically, the Court held that claims of overpaying for products and loss of personal information, on their own, do not support a finding of Article III standing.

On August 3, 2015, Neiman Marcus filed a petition for en banc review of the Seventh Circuit's decision on the grounds that the court's use of an "objectively reasonable" standard runs contrary to Clapper v. Amnesty Int'l USA, where the Supreme Court held that Article III harm must be "certainly impending."[9] In its July 20th opinion, the Seventh Circuit found that, unlike the phone records at issue in Clapper, the potential for hackers to cause consumer harm was more urgent.

In the States

California, Nevada Amend Definition of Personal Information in Data Security Laws

On July 14, 2015, the California legislature approved an amendment to the state's data security law.10 The amendment added health insurance information and username or email address to the statute's definition of "personal information," provided that the information elements are combined with a password or security question and answer that enable access to an online account. Health insurance information is defined to include insurance numbers, any unique identifier used by a health insurer to identify an individual, or any information in an individual's application and claims history, including any appeals records. This amendment brings the data security provisions of California law into line with the recent amendments to the data breach reporting sections of its code.

On July 1, 2015, Nevada's recently amended data security and breach notification law came into effect. The amendment, enacted on May 13, 2015, expands the definition of "personal information" to include a driver authorization card number, a medical or health insurance identification number, and log-in information for an online account, provided that these elements are unencrypted and are present in combination with an individual's first name or initial and last name.[11] The amendment exempts from the definition the last four digits of a driver authorization card number, but narrows the publicly available information exemption to information available in federal, state, or local governmental records. Companies have until July 1, 2016 to comply with the law as amended.

Illinois Governor Issues Conditional Veto of Bill Expanding State's Data Breach Law

On August 21, 2015, Illinois Governor Bruce Rauner vetoed Illinois Senate Bill 1833. The bill would have expanded the state's Personal Information Protection Act, a law that imposes a notification requirement on data collectors in the event of a security breach. Known as an "amendatory veto," the Governor's veto message was accompanied by specific recommendations to the legislative language that, if accepted by the legislature and the bill re-passed with such changes, it would be met with approval by the Governor and signed into law.

Introduced on February 20, 2015, the original text of SB 1833 would have added several categories of data to the definition of personal information, including geolocation data, consumer marketing data, and medical data. The bill would have added a requirement for data collectors to notify the state attorney general within 30 days if a breach affects more than 100 Illinois residents. The content and format of notification is specified in the bill. SB 1833 also contains a requirement for operators of websites to post a privacy policy, and includes a data security provision requiring data collectors to implement and maintain reasonable security measures to prevent unauthorized access, acquisition, destruction, use, modification, and disclosure.

In his amendatory veto, the governor rejected the inclusion of geolocation data and consumer marketing data in the definition of personal information on the grounds that such data "does not pose the same risk of identity theft that justifies" the costs and burdens of the notification requirement.[12] He also requested that the timeline for notification to the attorney general be increased to 45 days, and he recommended striking out the provision requiring website operators to post their privacy policies on the grounds that because California already had such a requirement, most large business already were compliant with this requirement on their websites.

[9] 133 S. Ct. 1138, 1147 (2013).

[10] California Assembly Bill No. 1541 *available at* http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1541.

[11] A.B. 179, 78th Sess. (Nev. 2015).

[12] SB 1833, Veto Message, 99th Gen. Assembly (Aug. 21, 2015), available at http://www.ilga.gov/legislation/99/SB/PDF/09900SB1833gms.pdf.

International

Russian Communications Ministry Clarifies Data Localization Law

On August 3, 2015, the Russian Ministry of Communications and Mass Media ("Ministry") took steps to clarify a data localization law that took effect September 1, 2015.

The data localization law, signed by President Vladimir Putin in July of 2014, requires the personal data of Russian citizens to be stored in databases that are located within Russia's borders. The data localization law applies to all companies that do business in Russia, including foreign entities.

According to guidance issued by the Ministry, the requirements of the data localization law apply only to entities that direct their business activities towards a Russian audience and make a deliberate effort to collect personal data. Evidence of directing business activities to a Russian audience include utilizing domain names such as .ru, .su, and .moscow, advertising in Russian or maintaining Russian translations of web content; and hosting online transactions in Russian currency.
The requirements of the data localization law are not retroactive, meaning that personal data collected from Russian citizens before the effective date can remain outside of the country as long as the data is not updated or changed. Further, the law does not limit remote access to databases in Russia, restrict the disclosure of personal data by Russian citizens for cross-border transactions, apply to non-resident entities, or apply to cross border data transfers, assuming the data collection originates in Russia.

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
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

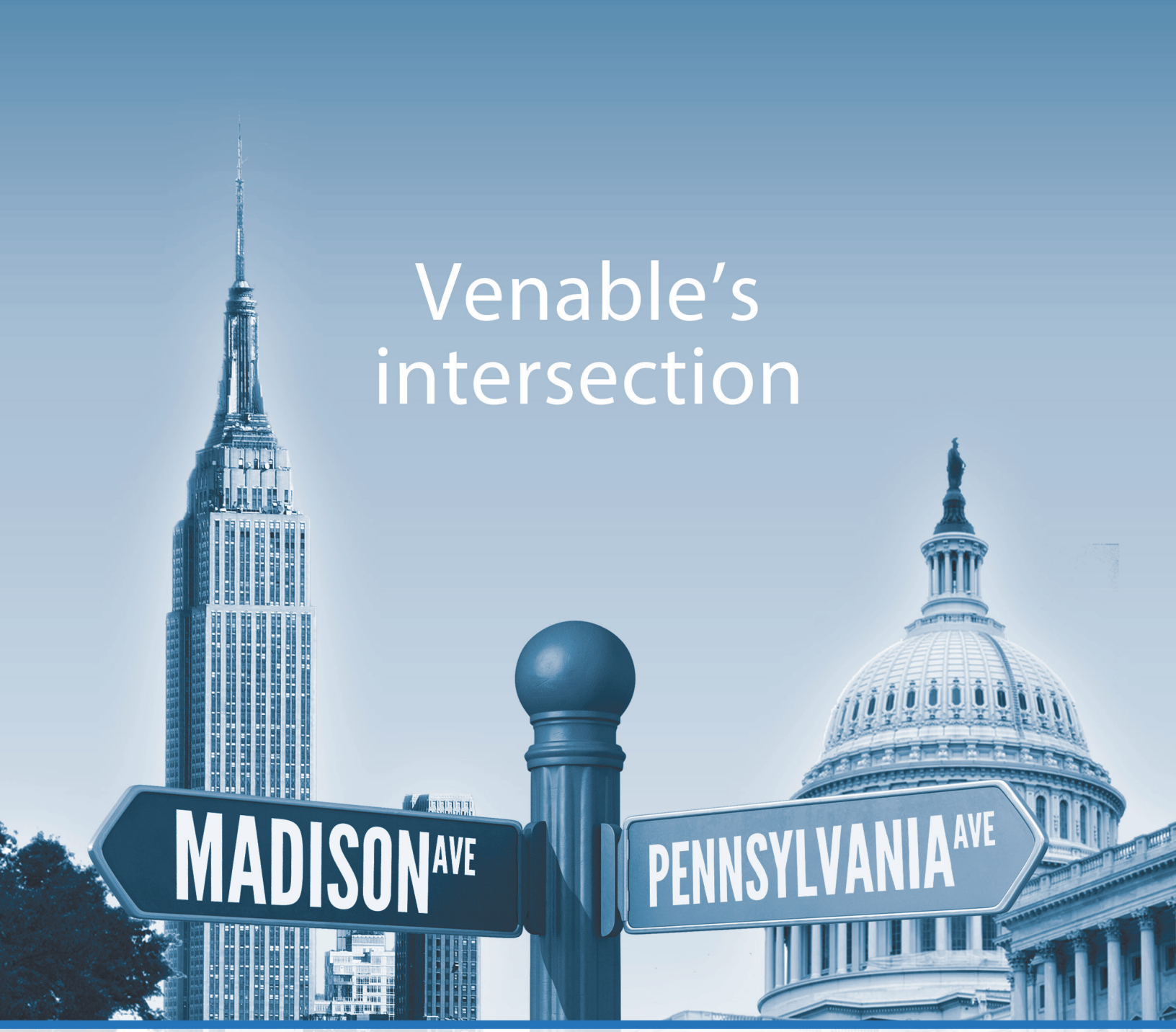
NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

SAN FRANCISCO, CA
505 MONTGOMERY STREET
SUITE 1400
SANFRANCISCO, CA 94111
t 415.653.3750
f 415.653.3755

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

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

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



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