July 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

Introduction:

In this issue, we review a number of federal agency developments, including the issuance of guidance by the Federal Trade Commission on data security practices, and by the Federal Communications Commission on the Telephone Consumer Protection Act. We discuss new laws enacted in three states addressing privacy and identity theft issues. On the international scene, we review legislative changes in Canada and privacy enforcement efforts in France. Finally, we include an announcement about new developments in Venable's State Attorney General Practice Group.

In this Issue:

Around the Agencies

FTC Releases Report on Data Security Practices Summarizing Enforcement Actions

On June 30, 2015, the Federal Trade Commission ("FTC") released a report entitled "Start with Security: A Guide for Business." [1] The report summarizes certain security practices that the FTC has identified in its more than 50 enforcement actions pertaining to data security. The report divides these security practices into the following categories: (1) collection, use, and disposal of personal information, (2) access control, (3) authentication practices, (4) encryption, (5) network segmentation and monitoring, (6) remote access, (7) product development, (8) service providers, (9) updating procedures, and (10) paper, physical media, and devices.

The report encourages businesses to adopt a number of security practices within each category. Specifically, the report recommends that businesses limit their collection of personal information to only that information for which they have a business need, that they dispose of personal information once they no longer have a business need for it, and that they substitute fictitious information for personal information whenever possible. The report also encourages businesses to limit access to personal information and administrative access to only those employees who have a business need for such access. The report further recommends that businesses implement strong authentication procedures, which should include developing a password policy that requires employees to use complex passwords, prohibiting the storage of user credentials in clear text, implementing a policy of suspending or disabling an account after repeated failed login attempts to guard against brute force attacks, and protecting against authentication bypass.

The report further recommends that businesses encrypt personal data from the moment they collect it until the moment they destroy it, use industry-tested forms of encryption, and make sure that the encryption is properly configured. According to the report, businesses should segment their networks so that they can provide increased security for particularly sensitive information, and they should implement intrusion detection technology so that they can identify and prevent attacks on the network. Businesses should also require that individuals with remote access to their network implement basic endpoint security, such as using a firewall and antivirus software, and they should limit the level of access that a third party can have within their network.

Additionally, the report recommends that businesses that develop products and services should ensure that their software engineers are trained in secure coding practices, that they follow the secure development guidelines set by the platform when applicable, that they verify that any privacy and security features work as intended, and that they test for common vulnerabilities. The report also encourages businesses to supervise the security practices of their service providers. Businesses are encouraged to incorporate appropriate security requirements into their contracts with third parties, and to conduct regular oversight of their service providers' security practices. Business should also regularly update their security with the timely implementation of software updates and patches and respond quickly to fix any publicly announced vulnerabilities. Finally, the report encourages businesses to protect paper records and portable media by securely storing records and devices, implementing secure transportation practices when transportation of portable media is necessary, and implementing secure data disposal procedures.

CFPB Releases Faster Payment System Principles

On July 9, 2015, the Consumer Financial Protection Bureau ("CFPB") released a set of principles setting out its vision for the consumer protections that should be incorporated into the development of faster payment systems. [2] The principles address a number of issues, including consumer control, fraud and error resolution, transparency, cost, and access, among others. They encourage businesses that are developing faster payment systems to clearly inform consumers about when, how, and the terms under which they have authorized a payment, to provide mechanisms for reversing erroneous and unauthorized transactions, to clearly disclose any fees, and to make the system broadly accessible.

The principles also highlight a number of best practices with respect to privacy and data security. Specifically, the principles encourage businesses to provide consumers with information—when such information will be helpful to consumers—about how their data is transferred through the payment system, including what data is transferred, who has access to it, how the data can be used, and its potential risks. The principles also encourage businesses to build into their systems protections to detect and limit errors, unauthorized transactions, and fraud. The principles call for such systems to allow gateway institutions to offer consumers enhanced security protections and limit the value of consumer payment credentials by implementing tokenization or other such tools.

---

1 FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

2 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CFPB'S VISION OF CONSUMER PROTECTION IN NEWER FASTER PAYMENT SYSTEMS (2015), *available at* http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf

National Telecommunications and Information Administration Announces Multi-stakeholder Processes for Drone Technology and Cybersecurity

The National Telecommunications and Information Administration ("NTIA") has announced the next steps in its planned multi-stakeholder processes for drones and cybersecurity. NTIA announced the first meeting of a multistakeholder process to develop best practices that enhance privacy and transparency around the operation of unmanned aircraft systems ("UAS"), *i.e.*, drones, by commercial and private users. Citing the wide range of innovative and beneficial services that UAS may provide, including news gathering, agribusiness, delivery, and providing internet in remote areas, the NTIA also cites the importance of consumer trust and responsible operation as the "keys" to expanding the potential uses of UAS. The first meeting is scheduled for August 3, 2015, in Washington, DC, with subsequent meetings planned for the fall.

Separately, NTIA announced a plan to launch its first cybersecurity multistakeholder process in September 2015. Following on the initiative announced by the Department of Commerce in March to address cybersecurity issues in the digital ecosystem, NTIA plans to focus this multistakeholder process on vulnerability research disclosure. NTIA's stated goal is to bring together security researchers, software and system vendors, academics, and other interested parties to create common principles and best practices around the disclosure of and response to security vulnerability information. The date and time of the first meeting have not yet been set, but it will be convened in the San Francisco Bay area in September.

Federal Communications Commission Issues Telephone Consumer Protection Act Guidance

On July 10, 2015, the Federal Communications Commission ("FCC"), by a 3-2 vote, published a Declaratory Ruling and Order ("Order") intended by the FCC to clarify what conduct violates the Telephone Consumer Protection Act ("TCPA").[3] The Order went into effect upon publication. Among other provisions, the TCPA requires prior express consent for certain autodialed and prerecorded/artificial voice calls and text messages to wireless numbers, and prior express written consent for telemarketing messages. Key points addressed in the Order included the following:

- The FCC affirmed that it considers the term "autodialer" to include technology with the potential capacity to dial random or sequential numbers, even if the technology does not have the present capacity or is not currently being used for that purpose.

- Regarding reassigned numbers, the Order permits companies to place one call to a reassigned number without obtaining the new subscriber's prior consent to receive autodialed calls, if the company had no knowledge of the reassignment and has a reasonable basis to believe that the company has the subscriber's consent; however, any additional calls will be considered a violation of the TCPA unless the company obtains the new owner's consent to receive autodialed/prerecorded calls.

- The FCC explained that consumers may revoke their consent to receive calls at any time and through any reasonable means, and the calling party may not limit the means by which a consumer may revoke their consent.

- The FCC recognized exemptions from the prior express consent requirement for specific types of financial alerts and healthcare messages, subject to certain conditions. This exemption does not extend to calls that include marketing or debt collection messages.

- The Order states that the TCPA does not prevent telecommunications companies or Voice over Internet Protocol ("VoIP") providers from providing consumers with technologies to block unwanted autodialed/prerecorded calls.

FFIEC Releases Cybersecurity Assessment Tool

On June 30, 2015, the Federal Financial Institutions Examination Council ("FFIEC") released a Cybersecurity Assessment Tool ("Tool") to aid financial institutions in identifying cybersecurity risks and to determine their ability to

3 In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 15-72 (July 10, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0729/FCC-15-72A1.pdf.

manage those risks. The Tool seeks to provide a repeatable process for institutions to assess their cyber preparedness over time by incorporating the FFIEC's Information Technology Handbook, the National Institute of Standards and Technology Cybersecurity Framework, and other regulatory guidance.

The Tool emphasizes the importance of engagement in cybersecurity planning and development by senior management of a company, including the chief executive officer and the board of directors. The Tool states that management should engage by developing assessments, supporting risk management plans, and overseeing modifications to those policies.

The Tool also contains two additional parts, the Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile is a methodology for allowing financial institutions to categorize levels of risk, from least inherent to most inherent risks. These risks could include delivery channels, mobile technology, and external threats. The Cybersecurity Maturity matrix ranks an institution's cybersecurity controls from Baseline to Innovative, supported by declarative statements. When taken together, the two parts of the Tool allow an institution to identify areas in need of improvement.

From the White House

White House Releases Proposed Privacy and Trust Principles

On July 8, 2015, the White House released proposed Privacy and Trust Principles ("Privacy Principles") for the Administration's Precision Medicine Initiative ("PMI"), a program that was announced by the President in his 2015 State of the Union address.[4] The proposed Privacy Principles are intended to help protect the privacy of individuals who volunteer their medical information for PMI.[5]

PMI is a federal research program that supports advancements in both science and policy that enable the development of individualized treatments for patients based on their specific characteristics, such as genetic makeup, environment, and lifestyle, as opposed to providing generalized treatments that are designed for the "average patient." The White House has stated that the success of PMI depends in large part on the ability of the initiative to protect and secure the individually identifiable health information that is volunteered and submitted.

The proposed Privacy Principles were drafted by an interagency working group that was co-led by the White House Office of Science and Technology Policy, the Department of Health and Human Services Office for Civil Rights, and the National Institutes of Health. The proposed Privacy Principles are intended to provide guidance on governance, transparency, reciprocity, respect for participant preferences, data sharing, access and use, data quality and integrity, and security.

The White House is soliciting public comments on the Proposed Principles through August 7, 2015.

In the States

Delaware Legislature Passes Privacy Laws

On June 25, 2015, the Delaware state legislature passed two bills addressing the issue of privacy: the Delaware Online Privacy and Protection Act, and the Student Data Privacy Protection Act. If signed into law, the Delaware Online Privacy and Protection Act ("DOPPA") would prohibit the marketing or advertising of certain products and services on Internet services directed to children.[6] The law's restrictions would apply to alcohol, tobacco, firearms, fireworks, tanning equipment, lotteries, drug paraphernalia, and certain types of body modifications, among others products and services. Operators of online services directed to children or operators who have actual knowledge that a child is using their service would be prohibited from using, disclosing, or compiling the child's personal information or allow others to do so, if the operator had actual knowledge the personally identifiable information ("PII") will be used for marketing or advertising the restricted products.

4 *See* https://www.whitehouse.gov/precision-medicine.
5 *See* https://www.whitehouse.gov/sites/default/files/docs/pmi_privacy_and_trust_principles_july_2015.pdf.
6 S.S. 1 for S.B. 68, 148th Gen. Assemb. (Del. 2015).

The bill would define PII to include a user's first and last name, physical address, e-mail address, telephone number, social security number, and any other identifier that "permits the physical or online contacting of the user." Operators who used an advertising service may shift compliance responsibility to the advertising service by notifying the advertising service that the operator's service is directed to children. DOPPA also would require operators who collect PII about users who reside in Delaware to conspicuously post their privacy policies and make certain disclosures. The law would direct the Consumer Protection Unit ("CPU") of the Delaware Department of Justice to promulgate rules regarding what information privacy policies must contain, and to provide sample language. The CPU would be required to make uniformity with other similar state laws a primary consideration when drafting such rules.

DOPPA also contains provisions applicable to the book information of book service users. A "book service" under the statute is a service allowing individuals "to rent, purchase, borrow, browse or view books electronically or via the Internet." The law would prohibit book service providers from disclosing a user's book service information to the government, absent certain delineated circumstances. Book service providers would also have to compile and post reports regarding the number of times book service information has been requested by the government and how many times the provider has disclosed it, among other data. The bill awaits action by the Governor of Delaware. If signed by the Governor, the bill would take effect on January 1, 2016.

The Delaware Student Privacy Protection Act ("DSPPA") is directed to operators (other than schools and school districts) of online services that are designed, marketed, and used primarily for K-12 school purposes.[7] The bill would require Operators to maintain reasonable security procedures and practices to protect student data and to delete student data within 45 days of a request from a school district or school. The security standards would, at a minimum, be required to comply with the Delaware Department of Technology and Information's Cloud and Offsite Hosting Policy. Under DSPPA, operators could not knowingly engage in targeted advertising based on student data, create student profiles based on information they collect, sell student data, or disclose student data absent an applicable exception. Operators would be permitted to use student data for maintaining, delivering, supporting, evaluating, or diagnosing their own services or for "[a]daptive learning or customized learning purposes," and would be able to use aggregate or de-identified data for their own marketing purposes.

SDPPA also awaits action by the Governor. If the bill is signed into law, the provisions restricting the actions of operators would take effect on the August 1 of the first full year following the act's enactment into law. All other provisions would be implemented immediately upon the Governor's signature.

Rhode Island Adopts Identity Theft Protection Law

On June 26, 2015, the "Rhode Island Identity Theft Protection Act of 2015" was signed into law. The new law requires state agencies, municipal agencies, and any "person" that "stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident" to create a security program with "procedures and practices…to protect the personal information from unauthorized access, use, modification, destruction or disclosure." The law requires agencies and businesses that share personal information of Rhode Island residents with a third party to have a written contract with the third party establishing security procedures and practices to safeguard the information.

Additionally, the law dictates that agencies and businesses must: have a written document retention policy; dispose of personal information after it has served the purpose for which it was collected; and destroy any information using a secure method such as incineration, shredding, or pulverization.

In the event of a data breach, the new law requires a breached agency or business to notify affected individuals within 45 days of breach confirmation. For any breach affecting more than 500 individuals, the breached entity must also provide notification to the Attorney General. Penalties for a violation of the Act may include monetary fines for reckless, knowing, or willful violations of the Act and a civil suit from the Attorney General. The law goes into effect June 26, 2016.

New Jersey Assembly Passes Bill Restricting Use of IDs by Retailers

On June 25, 2015, the New Jersey Assembly passed A.3946, the Personal Information and Privacy Protection Act, which aims to restrict the purposes for which a retailer may scan a customer's identification card.[8] The legislation would prohibit "retail establishments" from scanning a person's identification card, except (1) to verify a person's identity or the authenticity of the card when the customer pays with a method other than cash, returns or exchanges an item, or requests a refund; (2) for age verification prior to a sale of age-restricted goods or services; (3) for fraud prevention during a refund, return, or exchange, if the business uses a fraud prevention company or service; (4) to form a contractual relationship; (5) when required by state or federal law; (6) to send information to consumer

7 S.S. 1 for S.B. 79, 148th Gen. Assemb. (Del. 2015).
8 A. 3946, 216th Leg. (N.J. 2014).

reporting agencies, financial institutions, or debt collectors as permitted by federal law; or (7) for compliance with the Health Insurance Portability and Accountability Act ("HIPAA").

Under the bill, retailers would not be permitted to retain information collected for age and identity authentication purposes. Moreover, the bill would require that data collected for other purposes must be stored securely. In the event of a breach of security of this data, retailers would be required to notify the Division of State Police and affected individuals, pursuant to New Jersey's data breach notification statute. Retailers would be not allowed to share information collected pursuant to this statute with third parties for any purpose. The Senate has not yet acted on the bill.

International

Canada Passes Federal Data Protection Law

On June 18, 2015, the Canadian Parliament passed into law the Digital Privacy Act, or Senate Bill S-4, amending Canada's federal data protection statute, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), which applies to organizations engaged in business practices in Canada.[9] Certain features of the new law were in effect immediately following the bill's passage, except for provisions related to a mandatory data breach notification requirement, which will not come into effect until the Canadian government issues further regulations. An expected date for issuance of regulations related to the mandatory breach notification requirement has not yet been announced.

The new law's mandatory data breach notification provisions require organizations that are subject to PIPEDA to provide notification of a breach "as soon as feasible" to the Office of the Privacy Commissioner of Canada and potentially impacted individuals, and "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." The law provides a definition of "significant harm," which includes, but is not limited to, bodily harm, reputational damage, humiliation, financial loss, and identity theft. Additionally, the law requires each organization subject to PIPEDA to maintain a record of all security breaches involving personal information. The law imposes fines up to C$100,000 for any organization that knowingly violates these requirements.

The new law contains provisions that amend consent requirements under PIPEDA, including enactment of a graduated consent standard where consent is necessary if personal information is being used, collected, disclosed, accessed, or transferred. Among the exemptions to the new consent requirements are a business transactions exemption where organizations may, in certain, cases use, collect, access, or disclose personal information for business transaction purposes (*e.g.*, merger or acquisition), as well as certain circumstances where personal information is required for an investigation in connection with a breach of law, fraud, or a contract.

French Data Protection Authority sends enforcement notices to 20 websites for failing to obtain consent for cookies

On June 30, 2015, the French Data Protection Authority, the Commission Nationale de l'Information et des Libertés ("CNIL"), issued notices to 20 websites asking them to comply with the European Union's Cookie Rules ("Rules"). These letters follow one year after the CNIL conducted a "cookie sweep" of 24 spot checks, 27 online checks, and 2 hearings on the topic. The enforcement notices requested that companies come into compliance with requirements of the Rules within three months, or the company may face a fine of up to €150,000 for a first offence.

The CNIL's audit, in general, found that websites may have placed a banner informing website users about the use of cookies, but did not obtain the consent of the user before downloading a cookie onto a browser. Additionally, the CNIL found that the websites in question did not provide a valid mechanism to block or delete cookies. Specifically, the CNIL found that simply informing consumers that they can block cookies is not sufficient to meet the Rule's requirement to offer an effective and easily used tool to do so.

Finally, the CNIL noted that the Rules apply not only to operators of websites, but to all aspects of the online ecosystem, including advertising agencies. These notices indicate continued attention by European regulators to cookies, and the online advertising industry in general.

---

9 Parliament of Canada, Bill S-4, Second Session, Forty-first Parliament, 62-63-64 Elizabeth II, 2013-2014-2015.

Announcements

Senator Mark Pryor to Lead Venable's State AG Practice, Joined by Erik Jones, and Kevin Turner

Venable's State Attorneys General practice, which dates back decades and spans many industries, has recently been bolstered by the arrival of former Arkansas Attorney General and U.S. Senator Mark L. Pryor. In leading the practice, Senator Pryor is joined by Erik C. Jones, who served as former Assistant Attorney General and Director of the Policy Bureau for Illinois Attorney General Lisa Madigan, and Alabama's former Chief Deputy Attorney General Kevin L. Turner. Senator Pryor, Kevin Turner, and Erik Jones join numerous Venable practitioners who have years of experience representing companies of all sizes before state AG offices, often in high-profile, multifaceted matters.

Venable's State Attorneys General Practice offers a variety of practical and strategic solutions in dealing with the AGs, including:

- Building relationships and educating the state AGs and their teams about clients and clients' industries;
- Spending time with clients to help them develop their approach to the state attorneys general environment and trends, including providing political analysis and advice on a variety of business and litigation topics;
- Providing the substance and experience needed to handle practically any issue presented by a state AG working alone or alongside other state AGs;
- Working with clients to develop and execute strategies for AG inquiries, investigations, and litigation;
- Identifying emerging trends and working with clients to anticipate and proactively limit potential problems; and
- Engaging with AGs on behalf of clients regarding state and federal statutes, regulations, and policies.

With their unique set of backgrounds, Senator Pryor, Erik Jones, and Kevin Turner will work closely with the firm's eCommerce, Privacy and Data Security practice.

About Venable's Privacy and Data Security Team

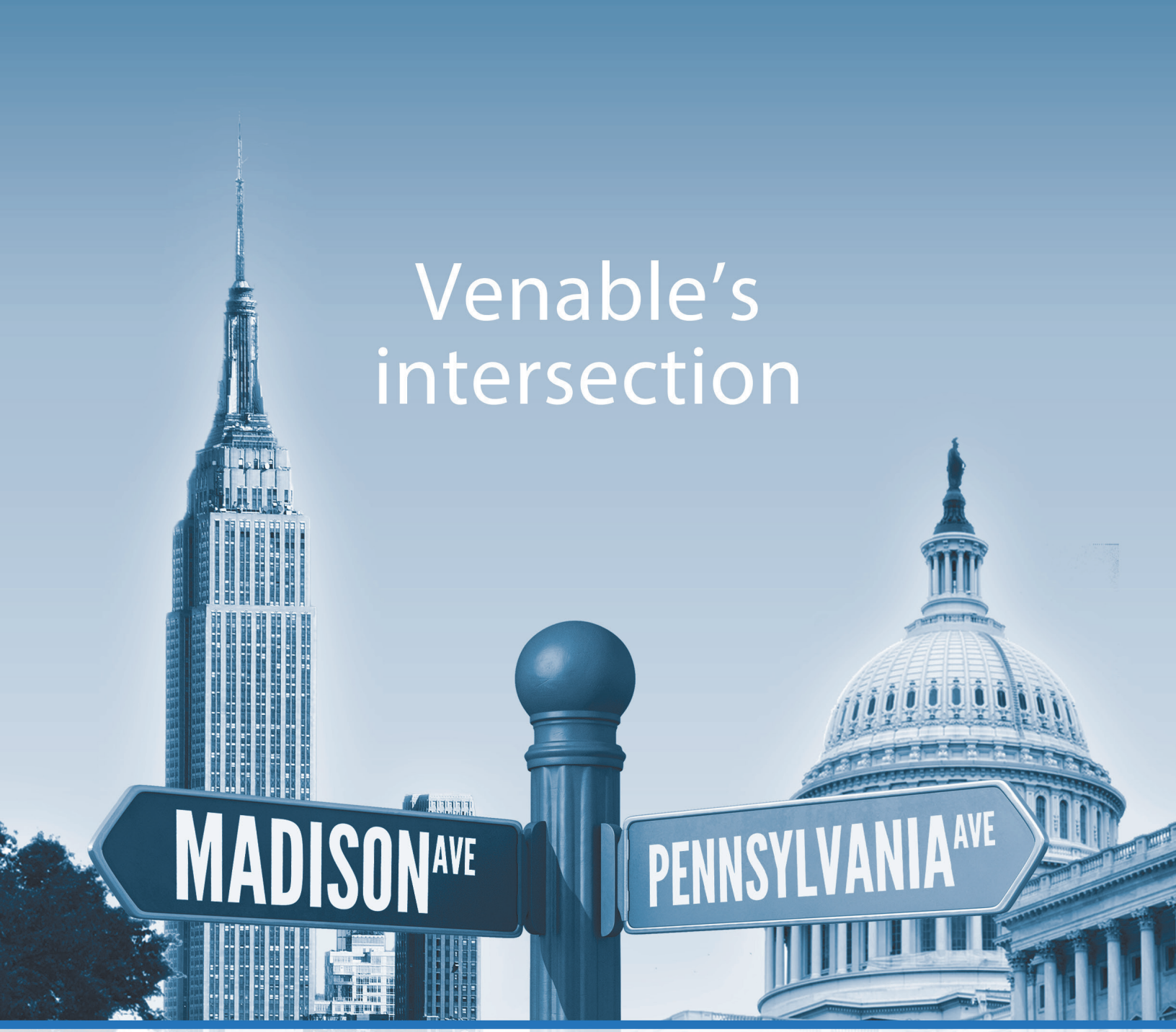
Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed 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	NEW YORK, NY	SAN FRANCISCO, CA	LOS ANGELES, CA	BALTIMORE, MD	TYSONS CORNER, VA
t 202.344.4000	t 212.307.5500	t 415.653.3750	t 310.229.9900	t 410.244.7400	t 703.760.1600



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