April 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 Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

Marissa Kibler

In this issue, we review developments on Capitol Hill, where Congress has been engaged on several privacy and data security issues, including the Internet of Things, driver privacy, and cybersecurity. In the Executive Branch and on the administrative front, we discuss the President's release of draft "Consumer Privacy Bill of Rights" legislation and the Federal Trade Commission's plans for a cross-device tracking workshop, among other notable developments. Finally, we review several international issues that have arisen, including the FTC's agreement with the Dutch Data Protection Authority.

In this Issue:

Heard on the Hill

Senate Passes Bipartisan Resolution on the Internet of Things

On March 24, 2015, the Senate unanimously passed a bipartisan resolution on the Internet of Things ("IoT") (*e.g.*, smart tablets, health wearables, smart home appliances).[1] The resolution, submitted by Senators Deb Fischer (R-NE), Cory Booker (D-NJ), Kelly Ayotte (R-NH), and Brian Schatz (D-HI), calls for a national strategy designed to maintain the United States as the global leader in IoT technology. The resolution expands on how the IoT can benefit consumers and advocates against the misuse of such technologies in a way that might hinder the evolving IoT landscape. Following a hearing on the IoT held by the Senate Committee on Commerce, Science, and Transportation a month prior, the resolution acknowledges existing and potential economic and consumer benefits of the IoT. Similarly, the Federal Trade Commission ("FTC") has also been focusing on the technology with the release of its IoT report earlier this year, which is in part based on a workshop the FTC held on the same topic in November 2013.

As part of the national strategy outlined under the Senate IoT resolution, recommended actions include: prioritizing IoT innovation, ensuring the recognition of businesses and other stakeholders in the development of a modern framework for IoT technology, deploying the IoT to help address current or future societal issues, and maximizing the use of the IoT across the federal government to curb waste, fraud, and abuse. In highlighting economic benefits of the IoT, the resolution states that the IoT "has the potential to generate trillions of dollars in economic opportunity" and can benefit the daily lives of consumers, including through public safety and healthcare. The resolution notes that IoT innovations can help businesses cut costs and maximize efficiency.

Senate Commerce Committee Holds Cybersecurity Risk Insurance Hearing

On March 19, 2015, the Senate Commerce, Science, and Transportation Committee's ("Committee") Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security ("Subcommittee") convened a hearing, entitled "Examining the Evolving Cyber Insurance Marketplace," to discuss the cyber insurance market and how cyber insurance might help companies address the growing threat of data breaches. Following hearings held by the Committee earlier this year on data breach notification legislation as well as on critical infrastructure cybersecurity, the hearing on cyber insurance was part of an overall effort of the Committee to further examine and address various cybersecurity issues. During the hearing, participants also weighed in on potential legislation regarding cybersecurity information sharing as well as a federal data breach notification standard. Witnesses who testified at the hearing included representatives from the insurance industry, government management, information technology, and academia.

Several potential benefits and challenges were raised by hearing participants with regard to the potential for cyber insurance to mitigate financial losses in the event of a breach. Subcommittee Chairman Jerry Moran (R-KS) stated that cyber insurance may provide an incentive for companies to adopt stronger cybersecurity practices since insurers may offer lower premiums to companies that carry a low security risk. Panelists agreed that cyber insurance can help companies reduce the costs associated with a breach and that companies may want to consider incorporating cyber insurance into an enterprise risk management plan as companies become increasingly vulnerable to cyber intrusions. An insurance industry representative noted that, while cyber insurance can help mitigate the losses that result from a breach, the potential scope of exposure cannot be covered by an insurance policy alone.

On cybersecurity information sharing, there was general consensus among witnesses and Subcommittee members that the federal government should assume a role in encouraging information sharing among private and public sector entities. A witness representing a government management company suggested that cybersecurity information sharing may help insurers develop more effective coverage and risk management solutions by enabling a further understanding of evolving cyber threats. Another possible policy solution raised was the enactment of a preemptive federal data breach notification standard, which witnesses agreed would help companies allay financial costs incurred by a breach.

Senators Introduce Legislation on Driver Privacy and EDR Data Ownership

On March 17, 2015, Senators John Hoeven (R-ND) and Amy Klobuchar (D-MN) reintroduced the Driver Privacy Act of 2015 (S. 766). This bill, like a previous version in the 113th Congress, would affirm that the data from a vehicle's event data recorder ("EDR") belongs to the vehicle owner. An EDR is a device that captures specific data in the event of a crash. The types of data

[1] S. Res.100, 114th Cong. (as passed by Senate May 24, 2015), *available at* https://www.congress.gov/114/bills/sres110/BILLS-114sres110ats.pdf.

collected may include vehicle speed at the time of impact; whether the brakes were applied; whether the airbag(s) deployed; crash forces at the moment of impact; the steering angle; and whether occupants were wearing seat belts. This data could be analyzed after a crash to help determine what the vehicle was doing before, during, and after the crash. Unlike a flight data recorder, EDRs do not record voice conversations inside the cabin or any vehicle location data. Furthermore, the EDR's recording period is limited to only 10-20 seconds prior to the crash event. Over 94 percent of vehicles are equipped with EDRs and in 2012, the National Highway Traffic Safety Administration ("NHTSA") proposed a rule that would require all automakers to include EDRs in their vehicles.[2]

While NHTSA's proposed rulemaking would not require any new data elements beyond what is already required by law, certain interest groups and policymakers have expressed concern over the privacy implications of EDRs. To that end, fifteen states have enacted statutes relating to EDRs and privacy, according to the National Conference of State Legislatures.[3]

The Senate bill would codify many of the data-related concepts from state laws, including clarifying that the owner of a vehicle is also the owner of any information collected by an EDR. Specifically, the bill would prohibit anyone other than the owner from accessing the data unless:

1. a court authorizes the retrieval of such data subject to admissibility of evidence standards;
2. the owner provides consent (most often for vehicle diagnosis, service, or repair);
3. the data is retrieved pursuant to certain authorized investigations or inspections of the National Transportation Safety Board ("NTSB") or the Department of Transportation;
4. the data is retrieved to determine the appropriate emergency medical response to a motor vehicle crash; or
5. the data is retrieved for traffic safety research.

Additionally, when data is retrieved in connection with traffic safety research or crash investigation, the bill would prohibit the disclosure of personally identifiable information and the vehicle identification number ("VIN"). Since there is no standard amount of time recorded prior to a crash, the bill would also direct the NHTSA to study the amount of time EDRs need to capture in order to provide sufficient information for crash investigations.

The U.S. Senate Committee on Commerce, Science, and Transportation approved the bill on March 25, 2015, with no amendments. The prognosis for floor action is unclear.

To help address concerns related to EDRs and other new vehicle-related technologies, a large number of auto manufacturers have committed themselves to privacy principles based on the Fair Information Practice Principles.[4]

From the White House

Administration Releases Draft "Consumer Privacy Bill of Rights Act"

In late February, the Administration released a discussion draft of a "Consumer Privacy Bill of Rights Act of 2015," a legislative proposal building on elements of the White House's 2012 consumer privacy report. As yet, Congress has not taken up the proposal.

Unlike existing federal privacy laws, the Administration's proposal is not specific to an industry sector or a certain data practice. The "Consumer Privacy Bill of Rights" recommends numerous new requirements on businesses related to the handling of personal data. "Personal data" covered by the legislation would include information linked or linkable by the entity controlling the data to a specific individual or a device associated with or routinely used by an individual, including, for example, unique device identifiers. De-identified data would be excluded from this definition.

Per the discussion draft, among other mandates, companies would be required to provide individuals notice of their privacy and security practices and a reasonable means to control personal data processing, with certain exceptions. A privacy risk

---

[2] The Federal Motor Vehicle Safety Standards: Event Data Recorders, 77 Fed. Reg. 240 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571).

[3] The fifteen states are Arkansas, California, Colorado, Connecticut, Delaware, Maine, Nevada, New Hampshire, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington.

[4] Additional information about the auto industry's privacy principles can be found at https://www.globalautomakers.org/media/press-release/automakers-commit-to-privacy-principles-to-protect-vehicle-personal-data.

analysis and mitigation steps would be required for any personal data processing that is not reasonable in light of "context" as defined in the proposal. Collection, retention, and use of personal data would also need to be reasonable in light of context, and personal data would be deleted, destroyed, or de-identified within a reasonable time after it is no longer needed for the original purpose of collection, with some exceptions to these rules. Certain security practices would also be required such as a risk assessment.

Further, if the discussion draft were to be introduced as legislation and enacted, companies would be required to provide reasonable data access to individuals upon request, to have procedures to ensure the accuracy of personal data (with some exceptions), and to provide a means for individuals to dispute the accuracy or completeness of personal data.

The proposal provides for enforcement by the Federal Trade Commission or state attorneys general, but does not contain a private right of action. Civil penalties totaling up to $25 million could be imposed for violations. However, the Administration draft would provide for a "safe harbor" from government enforcement through "codes of conduct" for personal data processing. Any person could submit a code for Federal Trade Commission approval or apply to administer and enforce an approved code of conduct.

Executive Order on Malicious Cyber Enabled Activities

On April 1, 2015, President Obama signed Executive Order 13694, titled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* (the "EO"). The EO declares malicious foreign cyber-attacks to constitute "unusual and extraordinary" threats to national security. The EO permits the blocking and seizure of all interests in property that are in the United States in response to such attacks. The actions authorized by the EO mirror the sanctions authorized against North Korean assets following the recent cyber attacks on Sony.

The sanctions permitted under the EO would apply to activity conducted outside the United States that have the purpose or effect of harming United States critical infrastructure (as defined by a presidential policy directive issued on February 12, 2013 outlining sixteen sectors of critical infrastructure, including energy, financial services, health care, and others); causing significant disruption to the availability of a computer or network; or causing misappropriation of funds or economic resources for commercial, competitive, or personal financial gain. These sanctions also extend to those making contributions to entities whose property is blocked, or that receive contributions from such people.

These sanctions are administered through the Department of Treasury, in consultation with the Attorney General and the Secretary of State. They would define entities as Specially Designated Nationals ("SDNs") and operate similar to existing sanctions administered by the Office of Foreign Asset Control ("OFAC"). The EO focuses on individuals and other non-state actors, as opposed to malicious cyber activity by a nation state. Similar to other sanction regimes, United States entities are prohibited from working with SDNs designated under the EO, as well as entities that are fifty percent or more owned or controlled by SDNs.

Around the Agencies

FTC Announces Cross-Device Tracking Workshop

The Federal Trade Commission ("FTC" or "Commission") has announced plans to convene a workshop on "cross-device tracking" on November 16, 2015 in Washington, D.C. The Commission has indicated that, with the advent of smart phones, tablets, wearable devices, and computers, the Commission's interest in how such data is combined—and now used—across devices is ripe.

The workshop is expected to focus on potential benefits and risks to consumers from the use of data collected across different devices for multiple purposes, including for marketing and advertising. At the workshop, the Commission has indicated that it will examine the following topics:

1. Do industry self-regulatory programs apply to cross-device tracking?
2. What are different types of cross-device tracking?
3. What information and benefits do companies gain from cross-device tracking?
4. What benefits do consumers receive from cross-device tracking?
5. What risks are associated with cross-device tracking?
6. How can companies make cross-device tracking more transparent and how can they give greater control to consumers?

Comments may be submitted to the FTC both prior to the workshop (until October 16, 2015) and after the workshop (until December 16, 2015).

Examination of the Commercial Use of Drones Continues

The last month has seen a variety of developments in the regulation of drones. The Federal Aviation Administration ("FAA") granted approval to certain companies to begin testing commercial drone use outdoors. Previously, companies that wanted to test drones were limited to testing them in indoor facilities. Testing still requires a licensed sport pilot to operate the drone. The approval is subject to strict limitations, including restrictions on flight height and speed as well as a prohibition on nighttime testing. The FAA also launched their new program for "fast-tracking" exemption requests to allow for more commercial drone development and testing. Under the new policy, the FAA may issue a blanket authorization for drone flights anywhere other than certain restricted areas—a change from the previous policy, which required that applications be made for particular blocks of airspace.

On March 24, 2015, the U.S. Senate Committee on Commerce, Science, and Transportation's Subcommittee on Aviation Operations, Safety, and Security held a hearing entitled, "Unmanned Aircraft Systems: Key Considerations Regarding Safety, Innovation, Economic Impact, and Privacy." Representatives from the FAA, the National Telecommunications and Information Administration ("NTIA"), and the U.S. Governmental Accountability Office ("GAO") testified, as well industry representatives. Companies pushed the FAA for faster approval of applications and more flexibility for testing beyond pilot's sight lines. Senators Ed Markey (D-MA) and Steve Daines (R-MT) raised privacy concerns, while Senator Cory Booker (D-NJ) suggested that many of the problems with drone use were associated with individuals, not commercial use. Senator Booker is expected to introduce legislation establishing temporary rules to allow flexibility for commercial drone testing.

Finally, as part of its "multistakeholder process," the NTIA sought comments regarding the development of privacy-related best practices for drones. Specifically, the NTIA raised questions regarding whether commercial drone use implicates special or heightened privacy concerns and how to craft functional best practices. The comment period closed on April 20, 2015, and the NTIA is expected to hold its first public meeting on drones by the end of May or early June.

Department of Commerce Seeks Comment on Cybersecurity Multistakeholder Process

The Internet Policy Task Force within the U.S. Commerce Department has requested public comments on potential cybersecurity topics to be addressed in a "multistakeholder process" similar to those that the Department has convened on several privacy issues. (*See* 80 Fed. Reg. 14360, Mar. 19, 2015.) Although the Commerce Department notice leaves room for a variety of different outcomes from the process, it confirms that compliance with any resulting document would be voluntary for companies. Comments are due by May 18, 2015.

The request for comment focuses on identifying key cybersecurity issues in the digital ecosystem, within a "definable area where consumers and organizations will achieve the greatest benefit and consensus in a reasonable timeframe." The notice solicits suggestions for security challenges that the multistakeholder process could address. In addition, the notice requests comments on a range of potential topics discussed in the notice: botnet mitigation; naming, routing, and public key infrastructure; Domain Name System, Border Gateway Protocol, and Transport Layer Security certificates; open source assurance; malware mitigation; web security; "malvertising" in which malicious code is served from legitimate ad networks; trusted downloads; cybersecurity and the Internet of Things; privacy and civil liberties implications of cybersecurity; managed security services; vulnerability disclosure processes; and security investment and metrics.

Finally, the notice asks what factors the Commerce Department should weigh in selecting issues for multistakeholder processes, and requests views on several questions related to how the multistakeholder process should be structured. Among other issues, the notice asks whether some topics may be better addressed by a single workshop or other event.

NIST Invites Public Comment After White House Cybersecurity Summit

The National Institute of Standards and Technology ("NIST") has invited the public to comment on the draft report it issued following the February 13, 2015, "Summit on Cybersecurity and Consumer Protection" convened by the White House and hosted at Stanford University. The NIST draft report, entitled "Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy: Summary and Next Steps,"[5] summarizes the workshop participants' key points and suggests areas for future cybersecurity efforts to be led by NIST. The comment period is intended to provide interested persons with an opportunity to provide feedback to NIST to help the agency prioritize future NIST projects.

The NIST draft report briefly summarizes the topics and challenges discussed at the workshop. One topic was how to protect privacy when consumers interact with retailers in ways enabled and enhanced by networked technologies. The draft report

[5] NAT'L INST. OF STANDARDS AND TECHN., NIST-IR 8050, EXECUTIVE TECHNICAL WORKSHOP ON IMPROVING CYBERSECURITY AND CONSUMER PRIVACY, SUMMARY AND NEXT STEPS (Draft 2015), *available at* http://nccoe.nist.gov/sites/default/files/NISTIR_8050_draft_final.pdf.

also highlights a number of data security topics, including challenges raised by increased technological access by third parties, by the rise of the decentralized workforce environment, and by consumers' adoption of new payment technologies. The draft report addresses whether and how stronger and more usable authentication might improve the security infrastructure around these challenges. In addition, the draft report identifies several principles related to data that were discussed at the workshop, such as the issue of data integrity. The period for comment on the draft report closes on May 17, 2015.

International

FTC Agrees to Future Cooperation with Dutch Data Protection Authority

In March 2015, the Federal Trade Commission ("FTC") signed a memorandum of understanding ("MOU") with the Dutch Data Protection Authority ("DPA") agreeing to enhance information sharing and enforcement cooperation on privacy-related matters.[6]

The MOU's stated objective is mutual assistance and the exchange of information for the purpose of investigating, enforcing, and/or securing compliance on practices that would violate applicable privacy laws of the respective countries that are the same or substantially similar.

As part of the mutual exchange of information, the MOU explicitly states that, among other actions, the United States and the Netherlands will share information, including complaints that may be relevant to investigations or enforcement proceedings; provide investigative assistance, including obtaining evidence on behalf of one another; exchange and provide relevant information to include self-regulatory enforcement solutions, technological expertise, and privacy and data security research; and coordinate enforcement against cross-border privacy violations. Requests from one country may be denied or limited based on the discretion of the responding country with explanation. The MOU also provides procedures for protecting the confidentiality of any information exchanged.

Previously, the FTC has signed similar documents with the DPAs in Ireland and the United Kingdom.

South Korea Passes Cloud Computing Act to Promote Private Cloud Services

On March 3, 2015, the Korean National Assembly passed the *Act on the Development of Cloud Computing and Protection of Users* (the "Act"). In addition to encouraging the public sector to use cloud computing, the Act establishes a set of data security guidelines for cloud service providers which will apply not only to Korean providers, but also to global cloud providers operating in the country. These guidelines include requirements to report data leakage to users, return or destroy certain user information at the end of a relationship, and disclose what countries' user information is stored in by the cloud service provider. Cloud providers are liable for damages if a breach occurs. The Act creates one of the only data security regimes to specifically differentiate cloud computing from other types of computing services. An enforcement decree is expected to be announced in April 2015, and enforcement will likely begin in September 2015.

Global Privacy Enforcement Network Releases First Annual Report

On April 1, 2015, the Global Privacy Enforcement Network ("GPEN") released its first ever annual report. The GPEN, established in 2010, facilitates cooperation among privacy enforcement authorities across the globe. The report highlights GPEN's growth, the tools that it has made available to its members, and its sweep examining the privacy practices of over 1,200 mobile applications.

On the topic of the GPEN's mobile applications sweep, the report stated that 26 privacy enforcement authorities participated in the sweep, which involved a review of the privacy practices of 1,211 mobile applications. Participating authorities examined the types of permissions requested, the relationship between the permissions requested and consumers' expectations based on the application's functionality, and the explanation provided to consumers addressing why the application needed to collect personal information. The report noted that the results of the sweep indicate that many mobile applications are requesting access to personal information without providing a sufficient explanation identifying the

---

[6] FED. TRADE COMM'N, MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES FEDERAL TRADE COMMISSION AND THE DUTCH DATA PROTECTION AUTHORITY ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR (2015), *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/150309ftcdutchcb-1.pdf.

use of such information. Following the sweep, twenty-three of the participating enforcement authorities sent a joint letter to seven major application marketplaces urging these marketplaces to require that each application having the ability to collect personal information must provide users with access to the application's privacy policy in a link in the application's marketplace listing.

Office of the Australian Information Commissioner Released Revised Guidance

On March 31st, the Office of the Australian Information Commissioner ("AIC") issued a revised set of guidelines pertaining to the Australian Privacy Principles ("APPs"). The APPs are contained in the Privacy Act 1988, which authorizes the AIC to issue guidelines to advise covered entities on the avoidance of acts or practices that interfere with—or have an adverse effect on—the privacy of individuals. The APPs set out standards, rights, and obligations with respect to the handling, holding, accessing, and correcting of personal information. The guidelines identify the requirements identified in the APPs, provide the AIC's interpretation of the APPs, and set out examples illustrating how the APPs may apply in particular situations.

In the revised guidelines, the AIC made six changes. First, the AIC clarified the circumstances in which small businesses are treated as organizations, making them subject to the APPs. Second, the AIC revised and expanded the discussion of when an entity carries on business in Australia, which is a component of the test for whether an APP entity has an Australian link. Third, the AIC updated the discussion of "sensitive information" to explain that information may be considered sensitive when it directly applies to or clearly implies an individual's racial or ethnic origin, political opinions, membership in a political association, religious beliefs, philosophical beliefs, sexual orientation, criminal record, health information, or biometric information. Fourth, the AIC modified the section pertaining to the circumstances under which an entity that is covered by the APP may be held responsible for the mishandling of information by its foreign service providers. Fifth, the AIC revised and expanded the discussion of when the international agreement exception to classification as an entity covered by the APPs applies. Fifth, the AIC clarified the examples of loss of, unauthorized access to, unauthorized modification of, and unauthorized disclosure of personal information.

About Venable's Privacy and Data Security Team

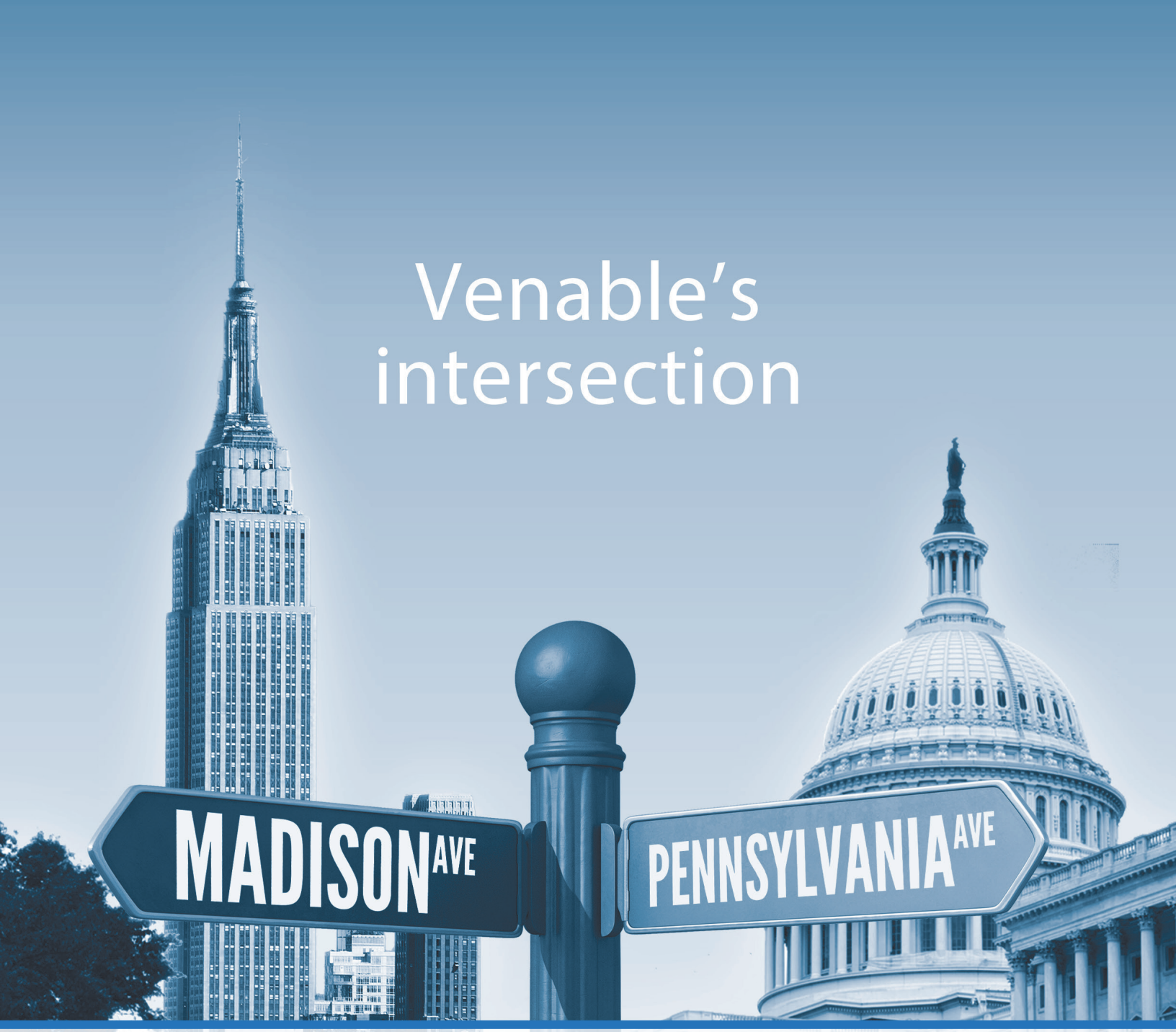
Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed 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.