December 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

David L. Strickland

Ari M. Schwartz

Erik C. Jones

Julia Kernochan Tama

Kelly A. DeMarchis

Tara Sugiyama Potashnik

Matt H. MacKenzie

Rob Hartwell

Emma R. W. Blaser

Sheena R. Thomas

Chan D. Lieu

POLICY ANALYSTS:

Marissa L. Kibler

London M. 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

In this Issue:

In this final issue of 2015, we review a number of developments on Capitol Hill, including hearings in the House of Representatives on ECPA reform, mobile payments, auto connectivity, and drones, as well as a House Energy and Commerce Committee markup of data security legislation and the enactment of a law related to privacy notices from financial Institutions. On the Executive and administrative side, we discuss the FTC's approval of a consent mechanism under COPPA and a Department of Commerce multistakeholder meeting on cybersecurity. Finally, we recap recent international developments related to the U.S.-EU Safe Harbor and a proposed data security and breach notification law for the EU.

Heard on the Hill

- House Judiciary Hearing on the Email Privacy Act
- House Energy and Commerce Hearing on Mobile Payments
- House Oversight Hearing on the Internet of Cars
- Drone Update
- House Financial Services Markup of H.R. 2205, the Data Security Act of 2015
- GLBA Privacy Notice Measure Enacted into Law

Around the Agencies

- NTIA Convenes Multistakeholder Process on Cybersecurity Vulnerability Research Disclosure
- NIST Seeks Comments on Use of Cybersecurity Framework
- FTC Approves Facial Recognition to Obtain Verifiable Parental Consent

Marketplace

- Digital Advertising Alliance Releases Guidance on Cross-Device Data Practice

International

- U.S.-EU Safe Harbor Update
- EU Lawmakers Reach Agreement on Cybersecurity Directive

Heard on the Hill

House Judiciary Hearing on the Email Privacy Act

On December 1, 2015, the House Judiciary Committee (Committee) held a hearing to discuss the Email Privacy Act (H.R. 699), a bill that would reform the way in which law enforcement agents can collect electronic communications and associated data from third-party electronic service providers during an investigation, currently governed by the Electronic Communications Privacy Act of 1986 (ECPA). Law enforcement agents, technology industry representatives, and privacy and civil liberties advocates discussed the need to modernize ECPA to accommodate technological advancements made in the 30 years since the law was enacted.

ECPA currently requires law enforcement agents to obtain a warrant for electronic information sought in the course of an investigation, but applies only to emails in transit or stored on a server for less than 180 days. The government is able to gain access to electronic information older than 180 days through a subpoena, which can be easier to obtain than a warrant. ECPA was passed before indefinite cloud storage of email was a common practice, which has led to a significant volume of electronic communications older than 180 days becoming available to law enforcement by means of a subpoena. It also distinguishes between messages stored in "electronic communication services" and "remote computing services," distinctions which were relevant in 1986 but lack application to modern communications networks.

In response to these issues, Representative Kevin Yoder (R-KS) introduced the Email Privacy Act, which would eliminate ECPA's different treatment of electronic communications stored for fewer than, or more than, 180 days, and ECPA's distinction between an "electronic communication service" and a "remote computing service." Regardless of the age or the type of service provider, the government would be required to obtain a warrant from a court before requiring providers to disclose the content of a communication. The bill also would amend existing law to prohibit a cloud services or email provider from knowingly divulging to a government entity the contents of any stored electronic communication without a warrant, and would revise provisions of ECPA under which the government may require a provider to disclose the contents of such communications. Other provisions of Rep. Yoder's bill would address procedural and notice requirements for the government upon obtaining a warrant, as well as other related measures.

During the hearing, witnesses expressed unanimous support for a digital information search warrant requirement but could not agree on the specifics of how to move forward. Representatives from civil and criminal law enforcement agencies expressed concern that the Email Privacy Act would limit their ability to investigate unlawful activity. Some advocates noted that in trying to keep pace with advances in technology, judicial interpretation of a technologically outdated law has harmed small businesses and created uncertainty around new technologies that rely on the use and storage of electronic information. Rep. Jerry Nadler (D-NY) asked how the bill would impact American businesses. An industry representative explained that the bill would help address the global misperception that the U.S. government has overly broad access to data held by U.S. companies.

The Email Privacy Act has 308 cosponsors. Committee Chairman Bob Goodlatte (R-VA) did not indicate whether he would recommend the bill for markup.

House Energy and Commerce Hearing on Mobile Payments

On December 1, 2015, the House Energy and Commerce Committee (Committee) Subcommittee on Commerce, Manufacturing, and Trade (Subcommittee) convened a hearing titled "The Disrupter Series: Mobile Payments." At the hearing, members and panelists discussed various applications of mobile payment technology, as well as security practices and data protection methods for mobile payments, such as multifactor authentication, encryption, and tokenization.

In his opening statement, Subcommittee Chairman Michael Burgess (R-TX) highlighted the widespread adoption of mobile payment technology and urged companies to continue to leverage a range of technologies to provide an easy and secure user experience for consumers. Subcommittee Ranking Member Jan Schakowsky (D-IL) discussed the growing popularity of mobile payment technology and raised concerns about the lack of consumer protection and adequate security practices in the industry. Committee Ranking Member Frank Pallone (D-NJ) noted that mobile payments are a welcome alternative for consumers who have limited access to banking and financial institutions.

In their questioning, members focused on security, data collection, and adoption of mobile payment technology. Subcommittee Ranking Member Schakowsky inquired about the type of data that companies collect from mobile payment transactions. An

industry representative responded that data collection varies widely across companies and noted that best practices for data security are still developing in the mobile payments industry. Committee Ranking Member Pallone inquired about protections for consumers who use mobile payments without a connection to a financial institution. A representative from academia suggested that consumers without access to financial institutions should have equal protection against fraudulent or criminal activities in the mobile payment space. Subcommittee Chairman Burgess, Subcommittee Ranking Member Schakowsky, and Representative Tony Cardenas (R-CA) inquired about how mobile payment technology can serve under-banked populations. An industry representative stated that under-banked communities stand to gain from the widespread adoption of mobile payment technology, especially in rural and densely populated urban areas, as mobile payment technology increases access to financial services.

House Oversight Hearing on the Internet of Cars

On November 18, 2015, two subcommittees of the U.S. House Oversight and Government Reform Committee – the Subcommittee on Information Technology and the Subcommittee on Transportation and Public Assets – convened a joint hearing titled "The Internet of Cars." The hearing focused on emerging automotive technologies involving vehicle-to-vehicle (V2V) communications, such as Dedicated Short Range Communications (DSRC), as well as potential cybersecurity and privacy concerns associated with connected cars. The panel consisted of government and industry representatives, including automobile manufacturers and cybersecurity professionals.

At the hearing, members and panelists noted the many potential benefits of connected cars, such as warning systems and automatic breaking systems, but also discussed potential cybersecurity and consumer privacy vulnerabilities that could stem from the emerging technology. Nat Beuse, Associate Administrator, Vehicle Safety Research at the National Highway Transportation Safety Administration (NHTSA), stated that NHTSA's approach to cybersecurity is focused on expanding its research plans and tools, facilitating industry self-regulation, developing new systems solutions, and considering mandatory minimum performance standards.

During the questioning period, the panel was asked about the potential need for automobile-specific cybersecurity legislation. A representative from the information technology industry stated that existing laws, like the Computer Fraud and Abuse Act (CFAA), already apply to hacking. Other panel members stated that there was no existing standard to prevent hacking. Vehicle manufacturers also described their current cybersecurity practices, including supplier audits and bug bounty programs to improve vehicle privacy controls. To close the hearing, Information Technology Subcommittee Chairman Will Hurd (R-TX) called on industry, not government, to develop privacy standards.

Drone Update

The use of unmanned aerial systems (UAS) continues to be an area of focus by Congress and federal agencies. On November 19, 2015, the House Energy and Commerce Committee (Committee) Subcommittee on Commerce, Manufacturing, and Trade (Subcommittee) convened a hearing titled "The Disrupter Series: The Fast-Evolving Uses and Economic Impacts of Drones." The hearing, which featured testimony from the UAS industry, technology services industry, and academia, focused on the risks and benefits surrounding UAS. In particular, Subcommittee members addressed the growing popularity of both commercial and recreational UAS, the difficulty integrating them into U.S. airspace, federal and state regulations, and safety issues.

On November 20, 2015, the National Telecommunications and Information Administration (NTIA) convened its fourth Multistakeholder Meeting to build a consensus around the privacy, accountability, and transparency issues associated with commercial and private uses of UAS. Stakeholders reviewed three different "best practices" documents to determine which draft should be used as a base framework going forward. The group selected two documents and is now working to reconcile the two drafts, which differ in several substantive ways, including with respect to how the best practices interact with First Amendment protections; restrictions on entering private property; and the scope of application of some privacy and security requirements. There is no timetable for completion of the reconciliation process.

The Federal Aviation Administration (FAA) also recently released its interim final rule addressing drone registration. Under the rule, operators of unmanned aircraft weighing under 55 and over 0.55 pounds will be required to register their drones online and pay a fee of $5. Operators can register as many UAS as they would like, but must label each UAS with the operator's contact information. Moreover, for accountability purposes, each UAS must display a unique identifier, which may be limited to the registration number provided by the FAA, or the FAA administrator may authorize the use of the aircraft's serial number. Registrations must be renewed after 3 years.

House Financial Services Markup of H.R. 2205, the Data Security Act of 2015

On December 8, 2015, the House Financial Services Committee (Committee) convened a full committee markup of H.R. 2205, the Data Security Act of 2015. Committee members weighed in on proposed amendments and certain elements of the legislation, including preemption of existing state data security laws, federal and state regulatory enforcement, and the scalability of data security measures to a business' operations and controls. In a 46-9 vote the following day, the Committee moved to report an amended version of the legislation out of Committee and to the House of Representatives. Two amendments were offered during the markup. The Committee voted to adopt a substitute amendment proposed by the bill's author, Representative Randy Neugebauer (R-TX). The other amendment, aimed at striking the preemption standard in the bill, was offered by Committee Ranking Member Maxine Waters (D-CA). Ranking Member Waters' amendment failed by a 26-20 vote.

The amended version of H.R. 2205 makes the following changes to the original text:

- addresses enforcement authority by state attorneys general where the Federal Trade Commission has not already initiated federal civil action,
- adds "within the most expedient time possible" to the timing of notification,[1]
- adds "State law enforcement agency" as a recipient of notification when appropriate,[2]
- removes the terms "substantial" and "inconvenience" from the definition of "harm" to consumers resulting from a breach that triggers notification,[3]
- removes "identity theft" and "financial fraud" from the list of types of harms covered,[4] and
- adds medical and health insurance information to the definition of sensitive information.

There was some disagreement among the Committee members on the scalability of data security measures in the bill and preemption. Rep. Mick Mulvaney (R-SC) suggested that the bill take into account the volume of consumer records held by a company. Rep. Waters noted her concerns regarding preemption, specifically mentioning that the bill would not provide state attorneys general with sufficient enforcement authority and would not address a private cause of action for individuals harmed by a breach. Rep. John Carney (D-DE), a sponsor of the bill, stated that there are other changes in the bill that he intends to propose in the future, based on his discussions with Rep. Waters. Reps. Neugebauer and Carney announced that they will continue discussions with stakeholders and lawmakers to address certain aspects of the bill, including the addition of a private cause of action, the role of state insurance regulators, and the collection of consumer information by regulatory agencies.

GLBA Privacy Notice Measure Enacted into Law

On December 4, 2015, the Eliminate Privacy Notice Confusion Act was enacted into law as part of a surface transportation reauthorization bill signed by the President that day.[5] The Eliminate Privacy Notice Confusion Act amends the Gramm-Leach-Bliley Act (GLBA) to provide certain exemptions to the requirement that financial institutions provide consumers with an annual privacy notice. The measure, introduced in January this year by Representative Blaine Luetkemeyer (R-MO), was widely supported by the financial services industry on the basis that it would reduce compliance costs associated with providing annual privacy notices.

Under the new law, a financial institution that does not share consumers' nonpublic personal information with unaffiliated third parties is not required to provide consumers with an annual privacy notice if the financial institution has not changed its information disclosure practices since its previous notice to that consumer. These financial institutions are permitted to share consumers' nonpublic personal information pursuant to certain exceptions under the GLBA, including those associated with disclosure to service providers or law enforcement, or as necessary to fulfill a transaction required by a customer. If a financial institution changes its privacy practices or discloses consumer information in ways inconsistent with these exceptions, the financial institution is no longer exempt from providing consumers with an annual privacy notice.

The Eliminate Privacy Notice Confusion Act continues the process of streamlining the delivering of privacy notices to consumers, which was initiated by the Consumer Financial Protection Bureau (CFPB) in 2014, when it issued a final rule permitting financial institutions subject to its oversight to post privacy notices online instead of issuing individual notices under certain circumstances. The law provides relief for financial institutions not subject to CFPB oversight.

---

[1] Amendment in the Nature of a Substitute to H.R. 2205, 114th Cong. (2015).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Fixing America's Surface Transportation Act, H.R. 22, 114th Cong. (2015).

Around the Agencies

NTIA Convenes Multistakeholder Process on Cybersecurity Vulnerability Research Disclosure

On December 2, 2015, the National Telecommunications and Information Administration (NTIA) convened its second meeting as part of a multistakeholder process dedicated to cybersecurity vulnerability research disclosure, the goal of which is to develop a shared understanding of the overlapping interests between security researchers and the vendors and owners of products discovered to be vulnerable, and to establish a consensus about voluntary principles to promote better collaboration. The multistakeholder process for cybersecurity vulnerability research disclosure is the first of several processes initiated by NTIA's Internet Policy Task Force in March 2015 that will be focused on cybersecurity in the digital ecosystem.[6]

Participants at the second meeting included representatives from technology companies, academia, automobile and medical device manufacturers, and security service providers. The group heard presentations from four working groups that were formed at the first meeting: (1) adoption and awareness, (2) multiparty disclosure, (3) safety and disclosure, and (4) economic incentives in the security industry. At the meeting, participants discussed various perspectives and the goals of industry stakeholders in response to the presentations, which included the circulation of discussion documents prepared by each working group.

At the meeting, technology company representatives from the working group on adoption and awareness focused their presentation on the current lack of adoption of security best practices. They suggested that a lack of education, finite resources, and the absence of personal accountability may be contributing to the limited adoption of security best practices. Government and industry representatives from the working group on multiparty disclosure discussed the complexity of vendor-to-vendor coordination, asserting that there is an absence of broad consensus on how to address vulnerability disclosures that affect multiple vendors because stakeholders generally disagree about how best to minimize risk. Suggesting that dependence on technology is increasing faster than the industry's ability to secure it, an industry representative from the safety and disclosure working group emphasized that consequences of security failures in either the auto industry or the medical device industry can result in physical harm. Representatives from industry and academia who participated in the economics and incentives working group noted both positive and negative incentives for parties to engage in vulnerability testing, including the economic benefits of early discovery and advanced defense systems, as well as the high cost and disruption of deploying patches to address security vulnerabilities.

The next meeting for the cybersecurity vulnerability research disclosure multistakeholder process will be held in February 2016.

NIST Seeks Comments on Use of Cybersecurity Framework

On December 10, 2015, the National Institute of Standards and Technology (NIST) issued a Request for Information (RFI) seeking input on existing uses of, and potential changes to, the voluntary Framework for Improving Critical Infrastructure Cybersecurity (Framework). The Framework, which was released in February 2014 following a year-long process involving stakeholders and government representatives, provides standards and guidance to help private and public organizations undertake cybersecurity risk management.

In the RFI, NIST has requested comment on the following issues:

- the variety of ways in which the Framework is being used to improve cybersecurity risk management,
- how best practices for using the Framework are being shared,
- the relative value of different parts of the Framework,
- the possible need for an update of the Framework, and
- options for the long-term management of the Framework.[7]

NIST states that the feedback will inform "planning and decision-making about how to further advance the Framework" and will be used in the development of an agenda for a workshop on the Framework, which is expected to take place at NIST's campus in Gaithersburg, Maryland on April 6-7, 2016.[8] The deadline for submission of comments in response to the RFI is February 9, 2015.

---

[6] Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360 (Mar. 19, 2015).

[7] *NIST Seeks Comments on Cybersecurity Framework Use, Potential Updates and Future Management*, National Institute of Standards and Technology (Dec. 10, 2015), http://www.nist.gov/itl/acd/20151210rfi.cfm.

[8] *Id.*

FTC Approves Facial Recognition to Obtain Verifiable Parental Consent

On November 18, 2015, the Federal Trade Commission (FTC) approved Riyo Verified Limited's (Riyo) application for approval under the Children's Online Privacy Protection Rule (the Rule) of a proposed verifiable parental consent method that involves the use of facial recognition technology. Riyo's proposed method, Face Match to Verified Photo Identification, requires that the parent take a picture of his or her photo identification, such as a driver's license or passport, using a phone's camera or a webcam. The authenticity and legitimacy of the photo identification are verified using computer vision technology, algorithms, and image forensics to ensure that the photo identification is authentic. Once the photo identification is authenticated, the parent takes a picture of his or her own face. The system ensures that the photo is of a live person and then uses facial recognition technology to compare the image of the parent's face to the image on the photo identification. If the system determines that the photos are a match, they are reviewed by a live agent. Once the verification process has been completed, the parent's identifying information is deleted.

In approving Riyo's proposed verification method, the FTC noted that it is very similar to an existing verification method under the Rule which verifies a parent's identity by checking a government-issued identification against a database. The FTC further stated that Riyo's proposed verification method is more rigorous than the existing method because it uses facial recognition technology to ensure that the identification was issued to the person who is interacting with the system. The FTC also noted that, like the existing method, Riyo's verification method requires the prompt deletion of the information submitted by the parent. The FTC concluded that the use of facial recognition technology to perform a one-to-one verification of the images submitted by the parent followed by review of the images by a trained professional is a sufficiently reliable method of verifying the parent's identity to satisfy the Rule's requirement for approval of a new parental verification method. The approval of Riyo's application marks only the second time that the FTC has allowed a new verifiable parental consent mechanism since the Rule was amended in 2013 to allow the FTC to approve methods of obtaining verifiable parental consent that are not currently enumerated in the Rule. The only other mechanism to obtain the

---

Marketplace

Digital Advertising Alliance Releases Guidance on Cross-Device Data Practices

On November 16, 2015, the Digital Advertising Alliance (DAA) released guidance, titled the Application of the DAA Principles of Transparency and Control to Data Used Across Devices (Guidance), to help companies apply the DAA Self-Regulatory Principles to the quickly expanding cross-device environment.[9] The Guidance makes clear that the transparency and control obligations of the current DAA Principles apply with respect to cross-device data practices, and are subject to the DAA's independent enforcement.

The cross-device guidance clarifies how the transparency and consumer control principles apply to browser and app-based opt-out choices made by consumers regarding how data collected on that browser or device may be used elsewhere, and how data collected on other browsers or devices may be used on the device where a choice was made. Like the DAA's Application of Self-Regulatory Principles to the Mobile Environment (Principles) – which went into effect in September 2015 – the cross-device Guidance when effective will be enforced by the DAA accountability programs.

A recent survey found that 79% of consumers aged 18-64 use at least three devices a day, representing a shift from a single screen to a multi-screen norm.[10] Keeping pace with innovation and changing consumer preference, the DAA convened an inclusive group of leading companies and associations in the digital advertising ecosystem to develop the Guidance as an initial step in applying the DAA Principles in the cross-device space. The Guidance represents another example of the DAA's adaptation to the ever-changing digital advertising space, as well as the flexibility of self-regulation to keep pace with the marketplace.

---

[9] The cross-device guidance is available for download at http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf.

[10] Vivian Chang, *Consumer Survey: Multi-Device Usage*, Advocate Market Research Bureau (July 2015), http://www.tapad.com/consumer-survey-multi-device-usage/.

International

U.S.–EU Safe Harbor Update

Delegations from the United States and the European Union continue to negotiate a new safe harbor agreement following the invalidation of the U.S.-EU Safe Harbor Framework by the European Court of Justice decision in early October. On November 16, 2015, EU Commissioner Vera Jourová made a public statement while visiting Washington, DC in which she expressed confidence that the parties would reach a new safe harbor agreement before the end of January 2016. She stated that U.S. companies should expect the agreement to create an oversight system that is more responsive and proactive, including stronger oversight by the Department of Commerce. She further stated that the agreement will include an annual review mechanism to address any concerns that arise.

On December 3, 2015, Commissioner Jourová again expressed optimism that a new agreement would be in place before the January deadline, stating that the EU and the U.S. have agreed on concrete next steps in order to come to a conclusion before the end of January 2016. However, Netherlands Justice Minister Ard van der Steur has expressed doubts that such an agreement will be reached in time, stating that the talks have yet to address national security issues.

On December 8, 2015, a group of U.S. and EU industry trade groups issued a joint letter to European and U.S. leaders. In it, they asked officials to take the following steps: (1) reach an agreement on a revised safe harbor agreement; (2) provide clearer guidance on the current legal situation; (3) preserve the single EU digital market; (4) establish a minimum six-month transition period before enforcement after the ruling; and (5) create "sound and predictable" data regulations under the EU's pending General Data Protection Regulation. On Thursday, December 10, 2015, Commissioner Jourová reported to the European Parliament's Civil Liberties, Justice and Home Affairs Committee regarding the status of safe harbor negotiations. She stated that any new safe harbor agreement will include a suspension clause that will allow the EU to suspend the agreement if it determines that certain conditions affecting the privacy of individuals' personal information exist.

EU Lawmakers Reach Agreement on Cybersecurity Directive

On December 7, 2015, representatives of the European Parliament and European Union governments agreed on the first EU-wide cybersecurity law, titled the Network and Information Security Directive (Directive).[11] The Directive is the result of a proposal put forward by the European Commission (EC) in 2013 to enhance network and information security.

According to the EC, the agreed-upon Directive would impose security and notification requirements on Digital Service Providers (DSPs), described as including search engines, eCommerce platforms, and cloud computing services. Similar rules also would be imposed on "operators of essential services," defined as including the transportation, energy, healthcare, and banking sectors. The Directive would require Member States to designate a "national competent authority" for implementing and enforcing the Directive, and would require these service providers to notify such authorities of any serious incidents related to cybersecurity.

The Directive also would require Member States to set forth a national cybersecurity strategy. It would also require each Member State to establish a Computer Security Incident Response Team (CSIRT) responsible for handling incidents and risks. The Directive would set forth measures to increase cybersecurity cooperation among Member States, such as through information exchanges and a network of CSIRTs. Finalization of the Directive will require formal approval of its text by the European Parliament and EC; the text has not yet been publicly released.[12] Member States will then have 21 months to implement the Directive and identify operators of essential services.

[11] Press Release, European Commission, Commission Welcomes Agreement to Make EU Online Environment More Secure (Dec. 8, 2015), http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[12] Press Release, Presidency of the Council of the European Union, First EU-Wide Rules to Improve Cybersecurity: Deal with the European Parliament (Aug. 12, 2015), http://www.eu2015lu.eu/en/actualites/communiques/2015/12/08-accord-nis/index.html.

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