May 2015

the download

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

VENABLE SNAPSHOT

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

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

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

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

ISSUE EDITORS:

Stuart P. Ingis
singis@Venable.com

Michael A. Signorelli
masignorelli@Venable.com

Ariel S. Wolf
awolf@Venable.com

ADDITIONAL CONTRIBUTORS:

Emilio W. Cividanes
ecividanes@Venable.com

David L. Strickland
dlstrickland@Venable.com

Julia Kernochan Tama
jktama@Venable.com

Kelly A. DeMarchis
kademarchis@Venable.com

Tara Sugiyama Potashnik
tspotashnik@Venable.com

Matt H. MacKenzie
mhmackenzie@Venable.com

Rob L. Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

In this Issue:

Heard on the Hill

Data Breach Notification Legislation Update

Multiple data breach notification bills are currently pending in both houses of Congress. H.R. 1770, the Data Security and Breach Notification Act of 2015, introduced by Representatives Marsha Blackburn (R-TN) and Peter Welch (D-VT) was reported favorably out of the U.S. House of Representatives Committee on Energy and Commerce on April 15, but has yet to reach the house floor.

Also on April 15, Senators Thomas Carper (D-DE) and Roy Blunt (R-MO) introduced S. 961, the Data Security Act of 2015, which sets a minimum data security standard and creates detailed federal breach notification requirements. On May 1, 2015, Representatives Randy Neugebauer (R-TX), Chairman of the U.S. House of Representatives' Committee on Financial Services, and John Carney (D-DE) introduced H.R.2205, the companion bill to S. 961. Senator Mark Warner (D-VA) has announced plans to introduce data security legislation that is expected to receive backing from the retail industry. Senator Warner's bill will be the third data breach bill to be introduced in the Senate this year. Senator Bill Nelson (D-FL) introduced the first bill in January.

On May 14, 2015, the House Committee on Financial Services ("Committee") held a hearing entitled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." The panel featured representatives from the financial services, retail, electronic transactions, and payment security industries. Topics discussed during the hearing include potential data security and breach notification legislation, payment technology (e.g., EMV, tokenization, encryption), and industry efforts to further protect consumers' financial information. During the hearing, representatives Neugebauer and Carney promoted bipartisan the Data Security Act of 2015.

Student Privacy Bills Introduced in the House and Senate

On April 29, 2015, H.R. 2092, the Student Digital Privacy and Parental Rights Act was introduced in the House by Representatives Luke Messer (R-IN) and Jared Polis (D-CO). The bill focuses on operators of online school services and has a stated purpose of providing privacy and data security protections to personally identifiable information.

H.R.2092 would prohibit targeted advertising on school services and the use of students' information for targeted advertising. The bill would not preempt state laws. Other provisions of the bill include: a prohibition on the creation of personal profiles of students for non-school related purposes; a requirement for operators to publicly disclose to schools the types of information they collect and how it is used; the imposition of data breach obligations on operators; and the granting of parents a right of access, correction, and deletion of their students' information. The bill that would allow school service providers to use information for adaptive or personalized student learning purposes. Such providers would also be permitted by the bill to use such information for improving operators' school services. The bill would give the Federal Trade Commission civil penalty authority under 15 U.S.C. § 57a(a)(1)(B). The bill has been referred to the House Committee on Energy and Commerce and the House Committee on Education and the Workforce, where it awaits further action.

In the Senate, a student privacy bill was also recently introduced. On May 13, 2015, Senators Edward Markey (D-MA) and Orrin Hatch (R-UT) unveiled S. 1322, the Protecting Student Privacy Act, a bill that was introduced previously in the 113th Congress. The stated purpose of the bill is to amend the Family Educational Rights and Privacy Act to help protect student data handled by private entities.

Among other provisions, S.1322 would: impose information security requirements on personally identifiable information from education records held by educational agencies and institutions as well as private companies; prohibit use or sharing of students' personally identifiable information for advertising or marketing; grant parents a right to access and correct their students' personally identifiable information held by private companies; require maintenance of a record of those who have requested or accessed students' education records; and promote data minimization and destruction policies. S. 1322 has been referred to the Senate's Committee on Health, Education, Labor, and Pensions, where it awaits further action.

Senate Committee Leaders Request GAO Study on Health Data Security

Following breaches affecting the healthcare industry, Senators Lamar Alexander (R-TN) and Patty Murray (D-WA), respectively the Chairman and Ranking Member of the Committee on Health, Education, Labor and Pensions, have submitted a request to the Government Accountability Office (GAO) for a study on the cybersecurity of health data. The senators asserted that current legal safeguards and standards have failed to prevent recent cyber attacks on healthcare information technology (IT) systems.

The senators asked the GAO to conduct a study focusing on five major topics: (1) cyber threats to health IT systems and their potential consequences; (2) whether any "gaps or ambiguities" exist in the current regulatory framework for health IT, including privacy and security rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA); (3) federal agencies' oversight and enforcement

of such privacy and security rules; (4) adoption by the health industry of cybersecurity standards from the National Institute of Standards and Technology; and (5) case studies of the effectiveness of selected organizations' privacy and information security controls for health data.

The request for a GAO study follows the formation of a bipartisan working group by the same senators earlier this year to focus on oversight of health IT security.

Senators Introduce Bill to Establish Interim Rules on Drones

On May 13, 2015, Senators Cory Booker (D-NJ) and John Hoeven (R-ND) introduced the "Commercial UAS Modernization Act" (S.1314), a bill that would establish a set of interim operating guidelines for commercial unmanned aircraft systems (UAS, or "drones") and make other changes to the law intended to promote the safe integration of drones into the national airspace system. The bill would preserve the Federal Aviation Administration's (FAA) rulemaking authority in this area and anticipates the issuance of final regulations by the agency. According to the sponsors' public statements, one motivation for the legislation is a concern that other countries are surpassing the U.S. in developing safety and operability rules for drones.

S.1314 would: (1) set forth interim guidelines for commercial use and testing of small UAS during the time that the FAA is finalizing rules; (2) build a framework for registering and using UAS for commercial purposes; (3) establish a deputy administrator position at the FAA with responsibility for safely integrating UAS in U.S. airspace and evaluating the impact of existing regulations; (4) establish a means of assessing the research and partnership capabilities of FAA test sites. The bill, which incorporates several provisions of the FAA's proposed rulemaking released in February,[1] has been referred to the Senate Committee on Commerce, Science, and Transportation, where it awaits further action.

Supreme Court Update

Supreme Court Grants Certiorari in Case with Implications for Privacy Litigation

On April 27, 2015, the United States Supreme Court granted certiorari in Spokeo, Inc. v. Robins—a case that could have longstanding implications for privacy litigation going forward. The case will be heard sometime during the Supreme Court's fall term.

The question presented in the case is whether Congress can confer, consistent with Article III of the U.S. Constitution, standing on plaintiffs who suffer no concrete harm, but have the ability to recover statutory penalties for violation of a federal privacy statute, in this case, the Fair Credit Reporting Act (FCRA).[2] The plaintiff, Thomas Robins, alleged that he suffered non-economic harm by the dissemination of information about him in violation of the FCRA. The defendant asserted that Robins lacks standing because he did not plead any actual injury.

Spokeo won in district court, but the Ninth Circuit reversed the district court decision.[3] The Ninth Circuit held that Robins met Article III standing injury requirements because statutory penalties are sufficient to confer standing without having to plead actual injury or damages. In doing so, the Ninth Circuit joined the Sixth, Tenth, and D.C. Circuits who had previously ruled similarly. The Second and Fourth Circuits have found to the contrary, and this circuit split led to the Supreme Court granting certiorari.

While the Supreme Court's decision will have direct impact on future FCRA litigation, it also holds broader implications for privacy suits generally. As several amici curiae have asserted in briefs, a number of privacy statutes including the Video Privacy Protection Act (VPPA)[4] and the Telephone Consumer Protection Act (TCPA)[5] provide a private right of action for alleged violations and statutory damages. Litigation under these statutes often fails because of the plaintiffs' inability to plead an actual "privacy" injury, quantifiable by damages

---

[1] Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9543 (proposed Feb. 23, 2015), *available* at https://federalregister.gov/a/2015-03544. A summary of the proposed rule can be found at http://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

[2] 15 U.S.C. § 1681 *et seq.*

[3] *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014).

[4] 18 U.S.C. § 2710.

[5] 47 U.S.C § 227.

Around the Agencies

Federal Communications Commission Holds Broadband Privacy Workshop

On April 28, 2015, the Federal Communications Commission ("FCC") hosted a public workshop on broadband consumer privacy to explore the FCC's role in protecting the privacy of consumer broadband Internet access services. In his opening remarks, FCC Chairman Tom Wheeler stated that the workshop had two goals: (1) to discuss how the FCC can ensure that section 222 of the Communications Act continues to protect consumers, and (2) to discuss how the FCC can promote a virtuous circle of innovation and investment.

The first panel discussed whether Internet service providers ("ISPs") should be regulated differently from other businesses that have access to consumer information. An industry representative suggested that, as a result of developments in technology and the ability to purchase consumer information from third parties, ISPs do not have any greater access to consumer information than any other entity. A consumer advocate on the panel disagreed, asserting that ISPs have a unique ability to collect information about their customers due to their role as the gateway to the Internet. The second panel discussed the application of Section 222 to broadband Internet access services. Several panelists encouraged the FCC to regulate ISPs in a manner that is consistent with the Federal Trade Commission's ("FTC") actions in this space. In response, an FCC representative stated that the Commission has been working closely with the FTC as it determines how to regulate broadband providers with respect to consumer privacy issues. The panelists also discussed how to define what constitutes customer proprietary network information, and what, if any, restrictions should be placed on acceptable uses of this information. The Commission has not announced plans with respect to further study of the privacy practices of consumer broadband Internet access services.

Federal Trade Commission Takes Action Against Retail Device Tracking Firm

On April 23, 2015, the Federal Trade Commission ("FTC") announced a settlement with Nomi Technologies, Inc. regarding the firm's retail tracking technology. Nomi provides technology to retailers to track consumer devices in a retail space. In its complaint, the FTC alleged that Nomi failed to offer consumers the ability to opt-out of tracking via an in-store mechanism, and that Nomi failed to provide adequate notice that tracking was taking place. The FTC alleged that Nomi failed to honor promises that it made in its privacy policy to notify consumers when a store uses Nomi's technology to track the consumer's movements and to provide an opt out mechanism that consumers can exercise in the store.

The FTC complaint stated that Nomi places sensors in retail locations that collect consumer device media access control ("MAC") addresses, device type, date and time of observation, and signal strength of the device. Nomi stores this information and uses it to track devices over time. Nomi delivers reports to retailers that identify how many consumers enter the store, how long their visits last, how many repeat customers come back to the store, and when customers visit other locations of the same chain. In the settlement, Nomi agreed not to misrepresent consumers' options for controlling when information is collected, used, or shared about them or their devices.

Department of Health and Human Services Releases Version 2.0 of Privacy and Security Guidance

On April 13, 2015, the Office of the National Coordinator for Health Information Privacy ("ONC") released version 2.0 of the Guide to Privacy and Security of Electronic Health Information ("Guide"). The Guide is designed to help small and medium sized businesses understand and comply with privacy and data security requirements under the Health Insurance Portability and Accountability Act ("HIPAA"). The Guide addresses obligations under the HIPAA Privacy Rule, notices of privacy practices, the HIPAA Security Rule, meaningful use, security management, breach notification, and enforcement. The newly revised Guide clarifies when someone is a business associate, discusses permitted uses of health information, and lays out steps for implementing a security management process. The Guide also provides questions that providers can use in assessing potential vendors' security practices and tips for using Certified Electronic Health Record Technology ("CEHRT") for HIPAA-compliant electronic communications with patients.

Department Of Justice Releases Cyber Guidance

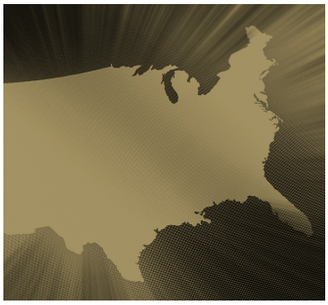
Last month, the Department of Justice ("DOJ") issued guidance on how organizations should prepare for and respond to information security incidents. First, the DOJ recommended that each organization perform an assessment of its data, assets, and services to determine which portions of its network require the most protection. Second, the DOJ recommended that organizations implement an incident response plan that:

- Identifies the person responsible for each element of the incident response effort;

- Provides contact information for all critical personnel and identifies how to proceed if critical personnel are unreachable;
- Indicates which mission critical data, networks, or services should be prioritized;
- Addresses how the organization will forensically preserve data related to the incident;
- Identifies the criteria the organization will use to determine whether data owners, customers, or partner companies should be notified if their data is affected; and
- Provides procedures for notifying law enforcement.

Third, the DOJ stated that organizations should conduct regular exercises to train employees on the incident response plan, and to make sure that the plan is current. Fourth, the DOJ recommended that organizations configure their servers to log network activity and obtain consent from network users to conduct real-time monitoring of the network. Finally, the DOJ encouraged organizations to identify legal counsel that is experienced in addressing issues associated with an information security incident and to establish a relationship with local law enforcement before a breach occurs.

The DOJ also recommended, that in response to an incident, organizations first assess the nature and scope of the incident and that the breached organization keep detailed records of the steps that it took to respond to the breach and the costs that it incurred. The DOJ further recommended that the organization forensically image the affected computers, preserve existing logs, consider increasing the size of its network log files, and develop a record of all steps that it has taken to respond to the breach. Breached organizations should also ensure that their employees are not using potentially compromised systems to communicate about response efforts and that their employees do not disclose information about the incident or the organization's response without verifying the identity of anyone seeking such information. Finally, the DOJ stated that organizations should not attempt to access, damage, or impair the systems that are being used as part of the attack as such efforts are likely illegal.



In the States

Montana Becomes 20th State to Limit Employer Access to Social Media Accounts

On April 23 Montana joined a growing group of states, now numbering 20 that have enacted laws restricting an employer's ability to require employees to allow access to their social media accounts. The Montana law prohibits employers from requiring a job applicant to:

- Disclose social media login credentials;
- Access social media accounts in the employer's presence; or
- Divulge information contained in social media accounts.

However, the law does not apply to social media accounts owned by the employer or provided to an employee for business purposes. Additionally, the law does not prohibit employers from gaining access to social media accounts to investigate:

- Workplace or criminal misconduct;
- Allegations of theft of confidential information and trade secrets, if there is specific information that such transfers are occurring; or
- Access needed to comply with federal laws and regulations.

Virginia passed similar legislation in March, with Connecticut and West Virginia failing to pass legislation on this topic in April. Two states, Mississippi and Wyoming, also voted down social media access legislation in February. 2014 saw 28 states introduce this type of legislation, with seven of those states enacting the bills into law.

Washington State Updates Data Breach Law

On April 23, 2015, Washington State enacted H.B. 1078, which amends Washington's data breach notification statute. Among other changes, the new law expands the statute's scope to cover paper files, adds certain content requirements for the notice to affected individuals, and adds an obligation to notify the Washington Attorney General for breaches involving more than 500 Washington residents. The new law also requires that notice to affected individuals be provided within 45 calendar days of discovering the breach unless an exception applies, authorizes the Washington Attorney General to enforce the statute, and expands the private right of action beyond "customers" to include "consumers." The bill will be effective as of July 31, 2015. Washington is the third state to amend its data breach notification this year along with Montana and Wyoming.

Virginia Becomes First State to Mandate Chip Payment Card Technology for State Agencies

Virginia became the first state to mandate the use of advanced chip authentication security features, i.e., "chip" payment card technology for state government agencies when Governor Terry McAuliffe signed Executive Directive 5 on May 5, 2015, entitled "Securing Consumer Transactions" (the "Directive").

The Directive instructs state agencies and merchants that accept payment cards from citizens to have in place chip technology no later than December 2015. It also instructs the Secretaries of Technology and Finance, the State Treasurer, and the State Comptroller to embrace electronic payment technologies that "meet or exceed" federal standards for the commonwealth's merchant, prepaid debt card, and purchase card programs. State officials are also required to provide a plan to the governor's office by October 1, 2015 detailing the Treasury's plans to enhance the security features of merchant and prepaid debit card programs to include user authentication, confidentiality, cardholder reporting of unauthorized withdrawals or suspected fraudulent transactions, and data breach reporting and notification. Separately, state agencies must also develop and adopt electronic identity management standards.

Gov. McAuliffe's actions follow the Executive Order signed by President Obama in October 2014 that mandated that all federally issued credit and debit cards employ enhanced security features including chip-and-pin technology. Unlike the federal Executive Order, however, the Virginia Directive only requires use of chip technology, not chip-and-pin.

Maryland, Florida Enact New Laws Regulating Drones

On May 13, 2015, Maryland Governor Larry Hogan signed into law SB 0370, the Unmanned Aircraft Systems Research, Development, Regulation and Privacy Act of 2015. The new law establishes the state government as holding the exclusive authority to regulate the testing or operation of unmanned aircraft systems (UAS) in the State of Maryland, preempting the authority of counties and municipalities. The law also requires the Department of Business and Economic Development, along with other specified agencies and institutions, to undertake a study of the benefits and concerns of UAS, and requires State and local government entities to review the use of UAS and issue a report to the Governor and General Assembly by December 31, 2018. The bill, which takes effect on July 1, 2015, passed with wide bipartisan support in the Maryland Legislature, receiving unanimous support in the Senate and only a single dissenter in the House of Delegates.

On May 14, 2015, Florida Governor Rick Scott signed into law SB 766, the Freedom from Unwarranted Surveillance Act. The law prohibits private individuals or the state government from using a drone to record without consent an image of private property or people on private property with the intent to conduct surveillance. Existing exceptions for law enforcement activity were expanded to include activities by property appraisers, utilities, aerial mappers, cargo delivery systems, and business activities licensed by the state. The law authorizes "aggrieved parties" to initiate a civil action and obtain compensatory and punitive damages and injunctive relief for a violation of the law. SB 766 takes effect on July 1, 2015.

Marketplace

Digital Advertising Alliance ("DAA") Announces Enforcement Date for Mobile Guidance

The Digital Advertising Alliance ("DAA") announced that its Mobile Guidance would begin to be actively enforced beginning on September 1, 2015. The announcement, made on May 7, stated the Mobile Guidance requirements regarding mobile cross-app, precise location, and personal directory data would be enforced by the Council of Better Business Bureaus ("CBBB") and the Direct Marketing Association ("DMA") against companies that collect such data for interest-based advertising after September 1. This means that companies subject to the Mobile Guidance should review their compliance status prior to the enforcement date.

The DAA released the Mobile Guidance in 2013 to inform companies how the DAA's Self-Regulatory Principles apply to the mobile environment. The Mobile Guidance applies the existing DAA principles of transparency and control to the collection, use, and sharing of covered data for certain purposes. To that end, DAA also released two new consumer choice tools for the mobile environment in February to facilitate compliance with the Mobile Guidance.

Trustworthy Accountability Group ("TAG") Launches Brand Integrity Program Against Piracy

The Trustworthy Accountability Group ("TAG") has launched its Brand Integrity Program Against Piracy. This voluntary program is intended to enhance the quality of the ad ecosystem marketplace by providing a certified means to help fight ad-supported Internet piracy.

Specifically, the program is designed to create trust in the Internet ad ecosystem by helping entities minimize the inadvertent placement of digital advertising on websites or other media properties that have an undesired risk of being associated with the unauthorized dissemination of materials protected by the copyright laws and/or illegal dissemination of counterfeit goods. The program uses independent third-party validators to certify advertising technology companies as Digital Advertising Assurance Providers ("DAAP"). These validators are now accepting applications from entities seeking to be validated as DAAPs.

To be validated as a DAAP under the program, a company must show it can provide other advertising companies with tools to limit their exposure to undesirable websites or other media properties by effectively meeting one or more criteria outlined in the Core Criteria for Effective Digital Advertising Assurance. Such criteria include:

- *Identifying "Ad Risk Entities" (AREs)*: Assessing and identifying websites or other media properties that have a discernible risk of facilitating the unauthorized dissemination of copyrighted materials and/or the illegal dissemination of counterfeit goods.
- *Preventing Advertisements on Undesired Ad Risk Entities*: Enabling advertisers and agencies to restrict the display of their advertising on undesirable sites or other media properties that do not meet each advertiser's or agency's standards.
- *Detecting, Preventing, or Disrupting Fraudulent or Deceptive Transactions*: Ensuring protocols and capabilities exist to find and limit ad placements on Ad Risk Entities that use fraud or deception to avoid the standards set by the advertiser or agency.
- *Monitoring and Assessing the Compliance of Ad Placements*: Detecting and reporting on Ad Risk Entities that are not in compliance with advertiser or agency instructions to allow remedial action to be taken.
- Eliminating Payments to Undesired Ad Risk Entities: Using technology and protocols to prevent payments to undesired sites and other media properties.

Entities successfully completing the validation process will receive the TAG "Validated Against Piracy" certification mark. Additionally, companies in the digital ad ecosystem that work with DAAPs may receive TAG's "Certified Against Piracy" certification mark.

International

European Commission Unveils a Digital Single Market Proposal

On May 6, 2015, the European Commission unveiled a long awaited "Digital Single Market Strategy" (the "Strategy")—a broad plan with the stated intention of breaking down barriers between European Union ("EU") nations in the hopes of moving from 28 separate national, digital markets to a single one.[6] The webpage unveiled along with the strategy, http://ec.europa.eu/priorities/digital-single-market/, cites economic figures that such a single market would create 3.8 million jobs and contribute 415 billion euros per year to the collective EU economy.[7]

The Strategy rests on three broad "pillars," with corresponding initiatives underneath. Under the first pillar--"Better access for consumers and businesses to digital goods and services across Europe"--the individual initiatives include enforcing consumer rules more rapidly and consistently; ending geo-blocking; and identifying potential competition concerns affecting European e-commerce markets. In support of that initiative, an antitrust competition inquiry into the e-commerce sector was launched simultaneously with the Strategy.

The second pillar--"Creating he right conditions and a level playing field for digital networks and innovative services to flourish"--highlights initiatives such as analyzing the role of online platforms such as search engines, social media, and app stores in the market; reinforcing trust and security in digital services, namely through the handling of personal data; and proposing an industry partnership in the area of cybersecurity. The third pillar--"Maximi[z]ing the growth potential of the digital economy"--is to include an initiative proposing a European free flow of data; and defines priorities for standards and interoperability in areas such as e-health.

While the Strategy is merely aspirational at this point, the EC has proposed to turn the initiatives into legislative proposals by the end of 2016. In the meantime, it will begin taking steps, such as the antitrust inquiry mentioned above, to further these goals without legislative language.

---

[6] A copy of the Strategy is available at http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

[7] See http://ec.europa.eu/priorities/digital-single-market/.

Canada Privacy Commissioner Issues E-Marketing Guidance and Tip Sheet for Businesses and Consumers

To assist with the implementation of Canada's new anti-spam law, the Office of the Privacy Commissioner of Canada ("OPC") recently released E-Marketing Guidance. The anti-spam law came into force on July 1, 2014 and amended the Personal Information Protection and Electronic Documents Act ("PIPEDA") regarding the collection, use and sharing of personal information. In particular, the amendments relate to "address harvesting." which is the use of computer programs to scrape websites and compile lists of electronic addresses. PIPEDA now requires consent for the collection and use of email addresses for marketing purposes. Entities who receive email addresses from third parties must ensure that the third party obtained the appropriate consents and can be held accountable if no consent has been given.

Along with the guidance, the OPC released tips for businesses and consumers regarding the new law. The tips for businesses include asking email address providers about their methods for collection, obtaining consent, and updating their lists, and the guidance that consumers should be able to withdraw consent for the use of their email addresses at any time. The tips also recommend documenting due diligence in writing. Tips for consumers include using the words "and" and "dot" in place of the symbols when posting email addresses online, creating separate emails for personal use and online activity, using caution when opening emails or attachments from unknown senders, and installing and updating security software from a reliable company.

New Turkish Law Allows Cross-Border Transfer of Electronic Personal Data

Previously, Turkish law prohibited the transfer of personal data obtained through electronic communications services from Turkey to other countries. After this prohibition was annulled through judicial review, the Turkish Parliament in April 2015 adopted a new standard for the electronic communications sector that permits the international transfer of personal data with the data subject's explicit consent. Reportedly, the new law also codifies several standards that previously existed in regulation, including a requirement to adopt security measures for personal data, a requirement to obtain informed consent to retain and access data in users' terminal equipment for purposes other than providing electronic communications services, a requirement for data subject consent or another legal basis in order to record or intercept electronic communications, and a rule that personal data may only be processed in good faith and as permitted by law.

About Venable's Privacy and Data Security Team

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

About Venable

An *American Lawyer* Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
t 202.344.4000

NEW YORK, NY
t 212.307.5500

SAN FRANCISCO, CA
t 415.653.3750

LOS ANGELES, CA
t 310.229.9900

BALTIMORE, MD
t 410.244.7400

TYSONS CORNER, VA
t 703.760.1600