February 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

Marissa L. Kibler

Introduction

This month's issue of the Download reviews a burst of legislative and policy activity surrounding data breaches, the "Internet of Things," and cybersecurity. The President announced several new legislative initiatives during a January 12 speech at the FTC, including a data breach notification proposal, a revised "Consumer Privacy Bill of Rights," recommendations for legislation concerning student data, and a proposal aimed at bolstering cybersecurity between the public and private sectors. In the State of the Union, the President also urged Congress to pass cybersecurity legislation. The White House also revealed that it's Summit on Cybersecurity and Consumer Protection, first announced back in October, would take place on February 13 at Stanford University.

The House of Representatives announced committee hearings on cybersecurity and breach notification as well as matters related to the Internet of Things ("IoT"), the latter coming as part of the announcement that Representatives Issa and Delbene would be forming a congressional Internet of Things caucus. These hearings will be held as Congress considers various legislative proposals from both sides of the aisle aimed at cybersecurity, breach notification, and privacy.

The FTC also released its report on the IoT this month, containing a summary of its findings from the November 2013 IoT workshop. The coming weeks will see further legal, policy, and self-regulatory developments in privacy and data security.

In this Issue:

Heard on the Hill

Congressional Hearings on Data Breach Legislation

I. House Energy and Commerce Subcommittee Hearing

On January 27, 2015, the U.S. House of Representatives Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade convened a hearing entitled "What are the Elements of Sound Data Breach Legislation?" The issues discussed during the hearing included preemption, notification timing and triggers, the definition of harm, penalties, and enforcement authority.

During opening statements, Subcommittee Chairman Michael Burgess (R-TX) commented that a federal breach notification bill should include uniform but flexible data security standards. He also noted that security standards and breach notification requirements for the health and financial sectors should be dealt with separately. Subcommittee Vice Chairman Leonard Lance (R-NJ) stated that a federal data breach notification bill should preempt relevant state laws. Subcommittee Ranking Member Jan Schakowsky (D-IL) offered support for a federal data breach notification standard, but noted that such a standard should allow states to enact requirements that go beyond the federal standard and to allow for enforcement by state attorneys general. Rep. Peter Welch (D-VT) stated that notice to individuals in the event of a data breach should only be required when the consumer could be harmed by the breach. Committee Ranking Member Frank Pallone (D-NJ) also stated that he would not support a federal data breach notification bill that weakened state requirements in those states with stronger standards than the federal bill.

Witnesses at the hearing discussed the costs that businesses incur as a result of their efforts to comply with a patchwork of state data breach notification statutes. They also discussed whether a federal breach notification statute should require that businesses provide notice only where the breach involves a risk of harm to consumers. The witnesses also discussed whether data security standards should be included in a federal breach notification statute, and the role of the states in enforcing data security standards.

II. Senate Commerce Subcommittee Hearing

On February 5, 2015, the U.S. Senate Commerce, Science, and Transportation Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security convened a hearing entitled "Getting it Right on Data Breach and Notification Legislation in the 114th Congress." The hearing featured testimony from several industry sectors, including retail, financial services, security, and information technology, as well as from Lisa Madigan, the Attorney General of Illinois.

In his opening statement, Subcommittee Chairman Jerry Moran (R-KS) underscored data breaches as a growing threat to consumers and businesses, and identified a number of key issues that the hearing would address with respect to legislation, including: (1) the implementation of basic data security standards; (2) a federal data breach notification standard's preemption of state standards; (3) the trigger for breach notification; (4) the inclusion of exemptions or safe harbors; and (5) the timeframe within which companies must provide notice of a breach.

Witnesses discussed whether a federal breach notice statute should incorporate specific data security standards, whether it should expressly preempt state breach notice statutes, and whether a federal statute should be modeled after stronger or weaker state statutes. The witnesses also discussed whether a federal statute should recognize existing sector-specific data security and breach notification requirements. Attorney General Madigan expressed her opposition to federal preemption of state breach notification statutes, and suggested that any legislation that includes express preemption should allow state attorneys general to enforce the statute. In response to questions, the panelists generally agreed that a specific timeframe to notify consumers would not be helpful.

Senate Homeland Security Hearing on Cybersecurity Information Sharing and Preventing Cyber Attacks

On January 28, 2015, the U.S. Senate Homeland Security and Governmental Affairs Committee convened a full committee hearing entitled "Protecting America from Cyber Attacks: The Importance of Information Sharing." Committee members and witnesses discussed potential legislative solutions to prevent future cyber attacks through enhanced cybersecurity information sharing and a federal data breach notification standard. Committee Chairman Ron Johnson (R-WI) announced that passing bipartisan legislation to reduce the threat of cyber attacks is a priority of the committee this year.

While there was broad agreement during the hearing on the importance of information sharing amongst the private and public sectors, participants held various positions on whether liability protection should exist for only business-to-federal government sharing, rather than for business-to-business sharing as well. Another issue that arose was whether companies should be granted exemption from the Freedom of Information Act when sharing information, some suggesting that such an exemption might help to prevent cyber criminals from collecting personal information once it is made public. Some participants suggested that personally identifiable information be narrowly defined and prohibited from being shared to mitigate the risk of a potential hack during the sharing process.

Certain private information sharing partnerships, including Financial Services Information Sharing and Analysis Center ("FS-ISAC"), were highlighted during the hearing as an important part of the overall effort to prevent cyber attacks. On breach notification legislation, witnesses expressed the importance of a federal standard in reducing costs for businesses of all sizes and speeding up the process of notifying affected individuals. With regard to the White House's recently announced cybersecurity legislative proposal, committee members said that they would consider the proposal as well as other legislative options presented by members of Congress.

From the White House

White House Legislative Proposals: Privacy, Data Security, Cybersecurity, and Broadband

During the week of January 12, 2015, President Obama delivered a series of speeches announcing the Administration's legislative proposals for privacy, data security, cybersecurity, and broadband, which the President later covered in his State of the Union address. The President started off the week at the Federal Trade Commission ("FTC"), where he presented his plans for the Consumer Privacy Bill of Rights, student privacy, and data security and breach notification. The second speech, on cybersecurity, took place at the U.S. Department of Homeland Security ("DHS"), followed by a third speech in Iowa on expanding access to broadband Internet. Some members of Congress and leaders of committees with jurisdiction over these issues have announced their willingness to work with the Administration to push bipartisan legislation.

Highlights of the Administration's legislative proposals and other related initiatives are as follows:

- **Personal Data Notification and Protection Act**. The proposed legislation would establish a national data security and breach notification standard that would preempt existing state laws, requiring a 30-day timeframe for notification of affected individuals after determination of a breach. The legislation would also expand law enforcement's authority to locate and prosecute cyber criminals.

- **Consumer Privacy Bill of Rights Legislation**. After the Department of Commerce's two-year collaboration with private and public sector entities in revising the Administration's Consumer Privacy Bill of Rights proposed in 2012, the updated Consumer Privacy Bill of Rights will include measures to ensure that entities are held accountable for personal information that has been compromised and consumers are made aware of how their data is being collected and used. The legislative proposal would also give consumers the right to know that personal data collected for one purpose cannot be used for another purpose.

- **Student Digital Privacy Act**. The proposed legislation would prohibit the use of student information for marketing purposes, including targeted advertising. In addition, the proposal would prevent companies from selling student data to third parties for non-educational purposes and the possible "profiling" of students after student data is collected by companies and third parties. Many of the same prohibitions included in the proposal are similar to the California student privacy law passed in 2014, which the President has publicly supported.

- **Financial Security**. The Administration will continue to encourage broad adoption of Chip-and-PIN technology across the public and private sectors by requiring the federal government to move to Chip-and-PIN. Other initiatives publicly supported by the Administration include IdentityTheft.gov, the FTC's webpage for consumers who have had their identities stolen, as well as financial private partnerships that provide consumers with free access to their credit scores.

- **Cybersecurity**. The forthcoming cybersecurity proposal would encourage business-to-federal government information sharing, as well as business-to-business information sharing. The proposal would grant certain liability protections, including for businesses that share information with the Department of Homeland Security's National Cybersecurity and Communication Integration Center ("NCCIC"). To receive liability protection, private entities would be required to remove unnecessary personal information before information sharing occurs and to adopt certain measures to protect any personal information that is shared. The Administration will convene a White House Cybersecurity and Consumer Protection Summit on February 13th to bring stakeholders and federal officials together to discuss enhancing cybersecurity information sharing and other privacy and data security practices and initiatives to further protect personal information and prevent cyber attacks.

White House to Convene Summit on Cybersecurity and Consumer Protection

On February 13, 2015, the White House will host the "White House Summit on Cybersecurity and Consumer Protection" at Stanford University. The Summit will include representatives from across government and industry, including consumer financial protection, communications, computer security, law enforcement, retail, and consumer advocacy. Panels will address topics such as public-private cooperation, improving cybersecurity practices at consumer-oriented businesses, increased security of payment technologies, information sharing, international law enforcement collaboration, improving authentication methods, and technical security. The Administration will work to advance its cybersecurity priorities, which include infrastructure, incident reporting, international collaboration, secure federal networks, and creating a more " cyber-savvy" workforce. In particular, the President is expected to use the Summit to advance his BuySecure Initiative which launched in October 2014. The BuySecure Initiative has three primary components: enhancing the security of payments across industry, improving resources for victims of identity theft, and encouraging public-private information sharing about compromised accounts.

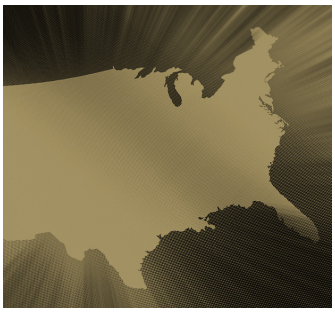
In conjunction with the White House Summit, the Department of Commerce's National Institute of Standards and Technology ("NIST") will co-host the "Cybersecurity and Consumer Protection Summit: Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy" with Stanford University on February 12, 2015. The workshop will feature speakers and panelists from both government and industry. The workshop's focus will be on the current challenges for consumer-facing industries in implementing cybersecurity and privacy technologies. The stated goal of the workshop is to create an "action plan" for addressing these challenges.

Around the Agencies

FTC IoT Report

On January 27, 2015 the Federal Trade Commission ("FTC") issued its long awaited report on the Internet of Things ("IoT") titled "Internet of Things: Privacy & Security in a Connected World" ("Report"). The Report was developed following a November 19, 2013, FTC workshop on the topic, and partially recapped the events of that workshop. The Report looked at both the potential benefits and risks created by the IoT, specifically looking at the applicability of the Fair Information Practice Principles ("FIPPs") to the space. While the Report did recommend against specific statutory regulation of the IoT, it also offered recommendations about applying the principles of (1) security, (2) data minimization, and (3) notice and choice to the IoT. These recommendations are focused on companies engaged in the space, with an eye toward addressing privacy concerns at an early phase in the industry's life cycle.

The FTC has signaled an increased focus on the IoT. Chairwoman Edith Ramirez commented on the topic in two public appearances, one at the Consumer Electronics Show ("CES") 2015 and another at the State of the Net Conference. At CES, the Chairwoman focused on the collection of data, the potential for unexpected uses of data resulting in adverse consequences, and risks to data security. Her suggestions to address these problems were: (1) adopting security by design, (2) engaging in data minimization, and (3) providing consumers with transparency and choice about unexpected uses. Echoing these statements, the Chairwoman commented on the IoT later in January at State of the Net. In these comments, the Chairwoman further discussed consumer choice, stating that the industry must innovate around how to deliver notice to consumers on devices with small or no screens, as well as the concept of data minimization.



In the States

New York Attorney General Seeks Heightened Data Security and Breach Standards

New York Attorney General Eric T. Schneiderman kicked off 2015 by announcing he would propose legislation to overhaul New York State's data security and breach notification laws. His legislative proposal would expand New York's data breach notification laws to broaden notification beyond the data elements traditional to state data breach notification regimes (social security numbers, state identification numbers, and financial account information) to include notification for breaches tied to "private information." Attorney General Schneiderman's legislation would define private information, in addition to the existing data elements, to include email addresses and passwords; an email address in combination with a security question and answer; medical information including biometric information; and health insurance information. These changes resemble similar provisions that became law in Florida last year and earlier amendments to California's data breach notification laws.

In addition, the legislative proposal would require any organization that collects or stores private information to implement reasonable data security measures. These measures would be required to include administrative, technical, and physical safeguards to protect private information. Organizations that obtain independent third-party audits and certifications annually showing compliance with New York law would have a rebuttable presumption of having reasonable data security for use in litigation.

The New York proposal also would include a safe harbor, intended to provide an incentive for organizations to adopt a heightened level of data security. Entities who wish to qualify for the safe harbor would categorize their systems based on the information they store, then develop an appropriate data security plan, and receive certification for their plan. Qualification for the safe harbor could potentially eliminate liability altogether. Keeping in line with a number of the federal cybersecurity proposals, the New York proposal would also incentivize companies to share forensic reports with law enforcement officials, by guaranteeing that such sharing would not affect any privilege and protection.

Attorney General Schneiderman expressed publicly his desire for New York to have the "strongest, most comprehensive" data security law in the country. Because Attorney General Schneiderman is unable to introduce legislation himself, he needs to attract a sponsor in the state legislature to introduce it for him. Early reports indicate that he is likely to find bipartisan support for the proposal, although it has not yet been introduced.

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

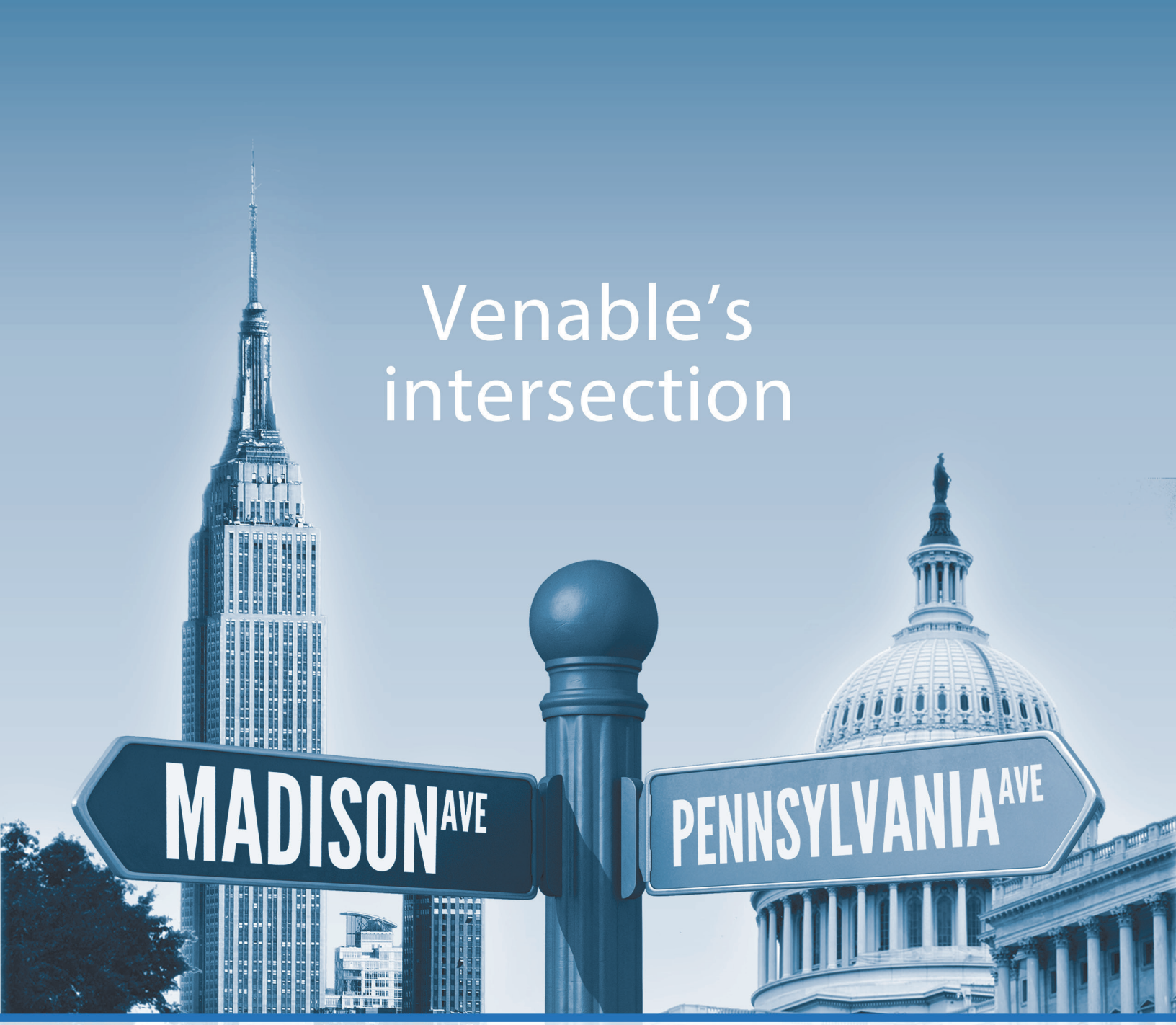
NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

SAN FRANCISCO, CA
SPEAR TOWER, 40TH FLOOR
1 MARKET STREET
SAN FRANCISCO, CA 94105
t 415.653.3750
f 415.653.3755

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

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

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



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