VENABLE LLP

the download

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

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Ariel S. Wolf
awolf@Venable.com
202.344.4464

Robert L. Hartwell
rlhartwell@Venable.com
202.344.4663
www.Venable.com

February 2014

In this Issue:

Heard on the Hill

Congress Holds Hearings on Preventing Data Breaches

In the aftermath of recent data breaches, the Senate Banking, Housing, and Urban Affairs' Subcommittee on National Security and International Trade and Finance, the Senate Judiciary Committee, and the House Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade conducted a series of hearings to examine potential solutions to prevent data breaches in the public and private sector.

Members of Congress and witnesses present at these hearings considered various tools to help prevent data breaches or otherwise respond to data breaches, including the expansion of the Federal Trade Commission's ("FTC") authority to regulate and enforce data security and breach notification measures and increased penalties on companies that knowingly conceal a breach. During and after these hearings, several members of Congress have announced their support for broad adoption of the "Chip and PIN" system to replace technologies that are more widely

used at point of sale ("POS") systems in the United States.

Senate Banking Subcommittee on National Security and International Trade and Finance

On February 3, 2014, the Senate Banking, Housing, and Urban Affairs' Subcommittee on National Security and International Trade and Finance ("Subcommittee") convened a hearing on data breaches entitled, "Safeguarding Consumers' Financial Data." The Chip and PIN system was repeatedly discussed throughout the hearing as a potential technology solution to help prevent hackers from obtaining unauthorized access to personal information from POS systems. Subcommittee Chairman Mark Warner (D-VA) stated his support for the Chip and PIN system, calling on the card industry and retailers to adopt the system.

Senate Judiciary Committee

On February 4, 2014, the Senate Judiciary Committee ("Committee") held a hearing on data breaches entitled, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." Senators present at the hearing agreed that recent data breach occurrences at retailers demonstrate a systemic issue that can only be addressed through collaboration from stakeholders and the government. During the hearing, Judiciary Chairman Patrick Leahy (D-VT) sought to draw support for his legislation, S. 1897, the Personal Data Privacy and Security Act of 2014. Senator Richard Blumenthal (D-CT) promoted his legislation, S. 1995, the Personal Data Protection and Breach Accountability Act of 2014.

House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade

On February 5, 2014, the House Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") held a hearing on data breaches entitled, "Protecting Consumer Information: Can Data Breaches Be Prevented?". Unlike the two Senate hearings on the same subject held earlier during the same week, this hearing waded into privacy issues as well. Representative Joe Barton (R-TX), Co-Chair of the Bi-Partisan Privacy Caucus ("Caucus"), stated that results from the hearing will supplement discussions in future Caucus meetings on such issues. Similarly, Representative Marsha Blackburn (R-TN) and Representative Peter Welch (D-VT), Co-Chairs of the Privacy Working Group ("Group"), noted that issues raised during the hearing will contribute to the dialogue during future Group meetings.

Around the Agencies

The NTIA Multistakeholder Process Continues

On February 6, 2014, the National Telecommunications and Information Administration ("NTIA") commenced a new multistakeholder process focused on facial recognition technology. Like the earlier NTIA multistakeholder process, which began in 2012 and focused on mobile application transparency, the purpose of the initial February meeting was to begin to develop a voluntary, enforceable code of conduct designed to provide transparency related to the use of facial recognition technology.

This meeting is the first of eight scheduled through June 2014.

Lawrence Strickling, Assistant Secretary for Communications and Information and Administrator of NTIA kicked off the meeting with remarks about the process' goal, which is to facilitate discussion on a path forward applying the White House's Consumer Privacy Bill of Rights to facial recognition technology in the commercial context.

The meeting featured three panels focused on the fundamentals of facial recognition technology, its commercial applications, and technical privacy safeguards.

The first panel featured panelists who provided information about the accuracy of the technology, and how it is currently applied, especially as used to determine age, gender, race, ethnicity, sexual orientation, and emotion. Audience questions probed the panel about the accuracy of matching photos to a database.

The second panel, which focused on marketing research and commercial applications of the technology, focused on its many positive uses. They explored how in marketing facial recognition technology can be used to gauge concepts such as emotional response, as well as improve accuracy by authenticating marketing participants. Other commercial applications touched upon were security and law enforcement. The audience focused on the use and sharing of this data.

Finally, the third panel discussed privacy safeguards over the data, including the risks arising from the linkage of offline data with online profiles. The audience focused on how notice would be provided to individuals about the use of facial recognition technology, as well as the limits of this technology and its potential for misuse.

On February 25, 2014, NTIA convened a second meeting of the facial recognition multistakeholder process. At this meeting, NTIA stressed that the process was focused on issues related to commercial use with the objective of drafting a private code of conduct. Facial recognition industry experts presented on key aspects of the technology, such as algorithms used to generate biometric templates and the error rates associated with the technology. During the facilitated discussion, participants discussed the size of databases used for matching as well as various factors that contribute to accuracy. At the end of the meeting, NTIA and participants agreed to conduct additional fact-finding at the next meeting in March, to be followed by an effort to begin drafting a code of conduct.

Department of Commerce Reports on U.S.-EU Safe Harbor Discussions

A delegation from the Department of Commerce ("Commerce") recently traveled to Brussels, Belgium to discuss the U.S.-EU Safe Harbor program with their European counterparts. The meetings centered on the thirteen recommendations for the Safe Harbor program issued by the European Commission ("EC") in a November 2013 report.

Commerce staff reported that the meetings focused mostly on the first eleven recommendations dealing with transparency, consumer redress, and enforcement, and did not delve deeply into the national security issues raised by the recommendations.

A series of meetings are being planned by Commerce to discuss all the recommendations, but with a greater focus placed on national security issues. These meetings are planned for Washington, D.C. through the spring.

FTC Holds Seminar on Mobile Device Tracking

On February 19, 2014, the Federal Trade Commission ("FTC") hosted a seminar entitled, "Mobile Device Tracking," as part of its Spring Privacy Series on emerging consumer privacy issues. The seminar included a panel of industry and consumer group experts on the emerging practice of device tracking. The panel covered the technical, legal, and policy challenges that will confront consumers and businesses in this new field.

After a presentation about the technology behind device tracking, questions about how retailers and marketers use the information gained from mobile devices were posed to the panel. The panel described various business and customer facing uses for the data, including faster checkout times, more efficient inventory management, and better theft prevention. The results of a recent study of consumer feelings toward sharing location data in exchange for deals or coupons was also released at the seminar, finding that 97 percent of Americans are willing to make such an exchange.

The seminar concluded with questions regarding the privacy implications of device tracking and the need for consumer notice. A distinction was made between app specific information and location data gathered from a device's antenna. Panelists discussed how device tracking companies collect information from the antenna, and not specific information from device applications. The panel cautioned against over-notification, and stressed the need to focus on the use of the collected data, not solely on how the data is collected. The FTC is expected to continue to study this space.

White House Developments

White House and NIST Release Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity

On February 12, 2014, the White House launched version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). The Framework was developed by the National Institute of Standards and Technology ("NIST") pursuant to Executive Order 13636, signed by President Obama in February 2013. The Framework was prepared in collaboration with industry stakeholders, and is presented as a guide to aid critical infrastructure companies in establishing and improving their cybersecurity programs.

The Framework closely tracks the draft that was released in October 2013. As with the earlier version, the Framework is still composed of the Framework Core, Profiles, and Implementation Tiers. Each component includes NIST recommendations for how to use and integrate the components and standards into a cybersecurity program.

One major change in the Framework is that the appendix discussing privacy and civil liberties has been integrated into a "Methodology to Protect Privacy and Civil Liberties" in the "How to Use" section of the Framework. Regarding the protection of civil liberties arising from cybersecurity activities, "direct responsibility" is limited to "government or agents of the government." As to "privacy implications," the Framework directs organizations to consider how a cybersecurity program "might incorporate privacy principles" such as data minimization, use limitations, individual consent and redress, and accountability. The Framework provides a list of processes and activities that may be considered as a means to address these principles. The announcement of the Framework was accompanied by the release of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity ("Roadmap"). The Roadmap provides a vision of how NIST hopes to improve the Framework overtime.

NIST will also begin the process of developing a privacy risk management model and technical standards. The goal of this process will be to identify and develop technical standards or best practices to mitigate the impact of cybersecurity on individual privacy. To begin this process, NIST will hold a privacy workshop in the second quarter of 2014 that will focus on the advancement of privacy engineering to aid in the development of privacy standards and best practices.

Venable News

NHTSA Administrator David L. Strickland Joins DC Regulatory Group

Top DOT official and former Senate committee counsel, who oversaw increased environmental and safety standards at NHTSA, joins Venable's highly rated group

Building on the strength of its Regulatory and Legislative practices, Venable LLP announced that David L. Strickland, Administrator of the National Highway Traffic Safety Administration (NHTSA), joined the firm's Washington, DC office as partner in January.

Nominated by President Barack Obama and confirmed by the United States Senate, Mr. Strickland has served as NHTSA Administrator since 2010. Through his position as the country's top automotive safety official, Mr. Strickland has overseen the development of the first national fuel efficiency program in conjunction with the Environmental Protection Agency, issued the first ever ejection mitigation standards for passenger vehicles to help keep passengers from being partially or fully ejected from vehicles during a rollover crash, and brought national attention to child passenger safety issues.

While at NHTSA, Mr. Strickland oversaw a broad range of vehicle safety and policymaking programs including setting vehicle safety standards, investigating possible safety defects, and tracking safety-related recalls; establishing and enforcing regulations on fuel economy; investigating odometer fraud and publishing vehicle theft data. He has also been a leader in the campaign to prevent distracted driving.

Prior to his tenure as the NHTSA Administrator, Mr. Strickland spent eight years on the staff of the U.S. Senate Committee on Commerce, Science and Transportation as Senior Counsel. Through this position he served as lead counsel for subcommittees overseeing the Federal Trade Commission (FTC), the Consumer Product Safety Commission (CPSC), NHTSA, and the Department of Commerce. Mr. Strickland provided legal and legislative advice to Members on a range of issues including insurance, antitrust, consumer protection and fraud prevention, internet privacy, tourism, consumer product safety and liability, passenger motor vehicle safety and fuel efficiency, and the U.S. Olympic Committee.

“An advocate for public safety on the roads, David has impressed the industry with his accomplishments,” said Brock R. Landry, co-chair of Venable’s Government Division. “From the Hill to the Administration, David is well respected and understands the often complex regulatory process from different points of view. He will play a key role in the ongoing growth of our Government Affairs, Automotive, and Technology practices.” Stuart P. Ingis, Partner-in-Charge of the Washington, DC office added, “David is a problem solver and consensus builder, both critical traits to effectively representing clients in Washington. David is a tireless advocate in everything he has done. We are thrilled to have him as part of the Venable team and I know he’ll bring the same passion and energy to our clients that he brought to his public service.”

Commenting on his move to Venable, Mr. Strickland said, “It has been an honor to focus on auto safety for the past four years, however, most of my work in public service has been on broad consumer protection policy, including FTC and CPSC issues. Venable has one of the strongest regulatory and consumer protection policy practices in America. Joining this team of extremely talented attorneys and experts to help develop cross-cutting and thoughtful solutions captures what I envisioned in a full service firm. I could not be more excited to be joining them.”

“With federal regulations impacting our daily lives in more ways than most people can imagine, Venable knows how to navigate through and how to get things done. I’m looking forward to this new challenge and bringing my experience to one of the top teams in the country,” he added.

At Venable, Mr. Strickland joins a bipartisan team of senior Washington insiders including former U.S. Senator Birch Bayh, former U.S. Secretary of Transportation James H. Burnley IV and former Congressman Bart Stupak. The team also includes former veteran Capitol Hill legislative staffers and Executive Branch policy advisors and regulators from both sides of the aisle.

Venable was recently recognized by U.S. News-Best Lawyers "Best Law Firms" as a Tier 1 firm Nationally and in Washington, DC for Litigation - Regulatory Enforcement (SEC, Telecom, Energy) and Tier 1 in Washington, DC for Administrative / Regulatory Law.

Mr. Strickland earned his J.D. from Harvard Law School in 1993 and a B.S. from Northwestern University in 1990.

****

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 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

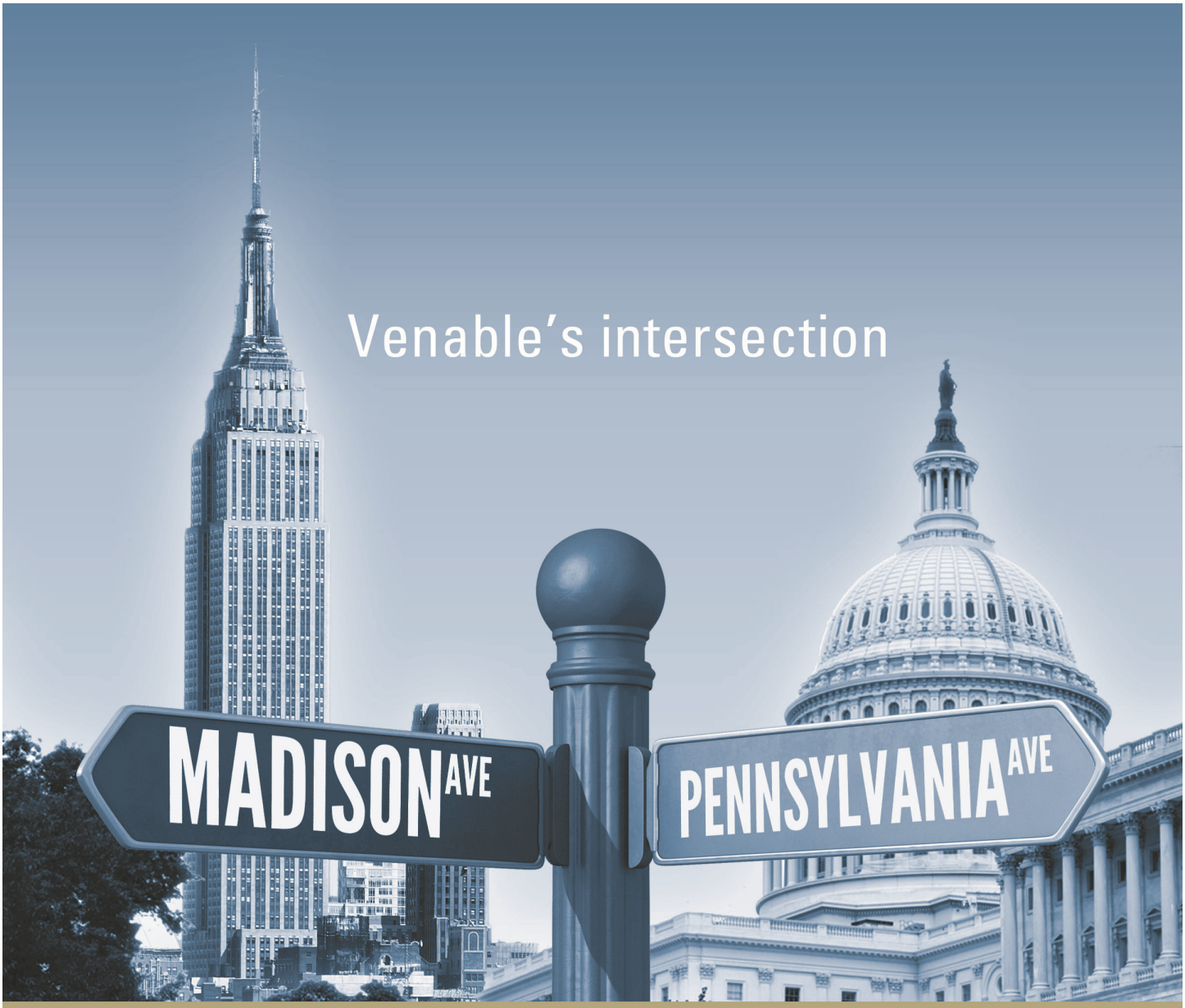
NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

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

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

SAN FRANCISCO, CA
SPEAR TOWER, 40th FLOOR
ONE MARKET PLAZA
1 MARKET STREEET
SAN FRANCISCO, CA 94105
t 415.653.3750
f 415.653.3755

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



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

VENABLE® LLP