October 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

Ari M. Schwartz
aschwartz@Venable.com

Erik C. Jones
ecjones@venable.com

Julia Kernochan Tama
jktama@Venable.com

Kelly A. DeMarchis
kademarchis@Venable.com

Tara Sugiyama Potashnik
tspotashnik@Venable.com

Matt H. MacKenzie
mhmackenzie@Venable.com

Rob Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Sheena R. Thomas
srthomas@venable.com

Chan D. Lieu
cdlieu@Venable.com

In this Issue:

In this issue, we review a number of congressional hearings that examined the data security and privacy aspects of vehicles, drones, and the sharing economy. We cover related developments in the White House and federal agencies, including an executive agreement with China on cybersecurity, an FTC workshop on data security, and an FCC meeting on robocall blocking. On the international front, we discuss the status of the U.S.-EU Safe Harbor Framework and other recent developments, including the European Commission's clarification on data retention. We also include an announcement about a new development related to Venable's Cybersecurity Services.

Heard on the Hill

House Energy and Commerce Subcommittee Holds Hearing on Vehicle and Roadway Safety

On October 21, 2015, the U.S. House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") held a hearing entitled "Examining Ways to Improve Vehicle and Roadway Safety." Topics included vehicle-to-vehicle ("V2V") communication technology, the recall process, and potential legislative solutions to enhance vehicle safety including the Subcommittee's "Discussion Draft on Vehicle and Roadway Safety" ("Discussion Draft"). Representatives of the National Highway Traffic Safety Administration ("NHTSA"), Federal Trade Commission ("FTC"), and various auto industry groups testified during the hearing.

The hearing focused on certain legislative proposals set forth in the Discussion Draft, including those pertaining to a safe harbor, incentives for vehicle manufacturers who deploy V2V technology in new cars, an advisory committee that would identify safety standards, and obligations for NHTSA regarding the recall process. The FTC highlighted its concern regarding the Discussion Draft's proposed safe harbor provision, stating that it is overly broad and may prevent FTC enforcement against vehicle manufactures who submit their privacy policies to the Secretary of Transportation. The FTC also warned that an advisory committee comprised of a majority of vehicle manufacturers may not establish effective cybersecurity best practices. NHTSA raised concerns that the Discussion Draft may limit NHTSA's authority in the creation of safety standards and recall notification process. With regard to incentives for deployment of V2V technology, Representative Jan Schakowsky (D-IL) emphasized her opposition to the proposal that would grant Corporate Average Fuel Economy credits to companies that adopt this technology. Auto industry representatives announced their support of the inclusion of V2V technology deployment in the Discussion Draft.

Subcommittee Chairman Michael Burgess (R-TX) asked auto industry representatives about existing industry efforts to address potential privacy and data security concerns regarding connected cars. Automaker trade groups highlighted the recently launched "Auto-Information Sharing and Analysis Center" and the "Consumer Privacy Protection Principles for Vehicle Technologies and Services" released at the end of last year. They also noted that certain automakers have pledged to adopt the National Institute of Standards and Technology Cybersecurity Framework and Automatic Emerging Braking Systems in new vehicles. Chairman Burgess stated that the Subcommittee will continue to collaborate with industry stakeholders and federal agencies to explore potential legislative solutions regarding recalls, as well as possible privacy and data security issues associated with connected cars.

House Judiciary Committee Holds Hearing on Unmanned Aerial Vehicles

On September 10, 2015 the U.S. House of Representatives' Judiciary Committee Subcommittee on Courts, Intellectual Property and the Internet convened a hearing entitled, "Unmanned Aerial Vehicles: Commercial Applications and Public Policy Implications." The panel featured representatives from a trade organization, the real estate sales industry, the insurance industry, and a consumer advocacy group. In his opening remarks, Subcommittee Chairman Darrell Issa (R-CA) highlighted the positive commercial and military uses of unmanned aerial vehicles ("UAV," or "drones"), while also expressing concern about regulatory inaction on the part of the Federal Aviation Administration ("FAA"). Judiciary Committee Chairman Bob Goodlatte (R-VA) stated that the Committee's interest in the subject stems from its longstanding jurisdiction over intellectual property and security issues, and that as the Committee studies the topic, it will specifically examine the technology's implications on privacy and security. Panelists made remarks on the beneficial uses of drones, including for inspecting and maintaining property as well as finding unique angles and views for photographing large structures, in addition to privacy and liability concerns.

In discussing privacy issues, some participants expressed concern about government surveillance and trespassing. The discussion also referenced the National Telecommunications and Information Administration's ("NTIA") multistakeholder process on unmanned aircraft systems ("UAS"), and the possibility that the process would result in a representative voluntary code of conduct. Subcommittee Ranking Member Jerrold Nadler (D-NY) called for a mandatory regulatory structure rather than a voluntary set of best practices that the NTIA process could provide.

Several panelists stressed the need for the FAA to finalize its draft rule on small UAS, citing difficulties with the current case-by-case exemption process that the FAA is using to allow the operation of small drones. There was discussion about the need for federal legislation to set rules for drone operation and use of airspace, and it was noted that state legislatures are attempting to fill what they view as a gap in federal law on the subject and consequently creating inconsistencies and a lack of certainty for drone operators. In his closing remarks, Chairman Issa noted that the hearing was one of a series of hearings that would likely take place across several congressional committees.

Subcommittee on Commerce, Manufacturing , and Trade Holds Hearing on the Sharing Economy

On September 29, 2015, the Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") of the U.S. House of Representatives Committee on Energy and Commerce held a hearing entitled "The Disrupter Series: How the Sharing Economy Creates Jobs, Benefits Consumers, and Raises Policy Questions." Members of the subcommittee and panelists discussed various policy challenges and consumer benefits of the sharing

economy. Subcommittee Chairman Michael Burgess (R-TX) focused his opening statement on the benefits of the sharing economy, advocating for small government and limited oversight to promote innovation. Ranking Member Jan Schakowsky (D-IL) warned that the sharing economy presents several challenging policy issues, and raised concerns about labor protections and data collection practices.

Panelists touted the benefits of the sharing economy including greater consumer choice and lower prices, and also suggested that consumer protection is built into sharing economy platforms through ratings and GPS location tools. Panelists also advocated for greater clarity in tax, insurance, and labor policy to better accommodate innovation in the sharing economy. Members focused their questions on the benefits of the sharing economy, and issues pertaining to labor and consumer protections. Chairman Burgess and panelists engaged in a discussion about the dynamics of supply and demand in the sharing economy, while Ranking Member Schakowsky asked about collective bargaining in the sharing economy. Congressman Frank Pallone (D-NJ), Ranking Member of the full Energy and Commerce Committee, voiced concerns about data security and privacy in the sharing economy.

From the White House

United States and China Reach Agreements on Cybersecurity

As one outcome of discussions between President Obama and Chinese President Xi Jinping during the latter's recent visit to the United States, the two countries have agreed to greater cooperation in the area of preventing cybercrime and intellectual property theft. White House materials on the agreement highlighted four aspects of the mutual commitments.

First, each country committed to responding in a timely fashion to information requests related to cybercrime, to cooperate with requests to investigate and mitigate cyber activities from their territories, and to update the other country on such investigations. Second, each country agreed not to "conduct or knowingly support" intellectual property theft, through cybercrime, that is intended to provide competitive advantages to certain companies or sectors. Third, each country stated its commitment to advance, within the international community, norms of national behavior in cyberspace. Toward this end, the countries agreed to create a senior experts group.

Finally, the countries committed to a "high-level joint dialogue mechanism" on cybercrime and other related issues, to be launched before the end of 2015 with semi-annual meetings thereafter. In the United States, this mechanism will be led by the Attorney General and the Secretary of Homeland Security with input from other law enforcement and intelligence bodies. The purpose of this group would be to review each country's responses to cybercrime information requests by the other country. A hotline will be created for escalation of issues with information request responses.

Around the Agencies

FTC Holds Workshop on Data Security

On September 9, 2015, the Federal Trade Commission ("FTC") held a workshop in San Francisco, California entitled "Start with Security." FTC Chairwoman Edith Ramirez opened the workshop by stating that the FTC expects businesses to implement reasonable security measures and to truthfully represent their security practices. She also cautioned that security best practices should not be overlooked in the rush to innovate. The panelists, which included representatives from several technology companies and security firms, discussed how companies could focus on security at the beginning of product development and the importance of a commitment from upper-level management to creating a security-focused culture. Panelists also encouraged companies to implement basic penetration testing, source code review, and threat modeling, although there was some discussion on whether companies should focus on security training and building security into information systems before seeking out penetration testing services.

Several panelists further discussed the need for a strategic approach for addressing vulnerabilities. They asserted that companies should have a contact point for outside individuals to report vulnerabilities, and they should dedicate appropriate resources to responding to vulnerability reports to enable timely identification of valid reports. One panelist commented that companies may be able to encourage vulnerability reporting by providing public acknowledgement instead of providing cash incentives. He further noted that companies should not encourage researchers to target actual customer data. A second workshop will be held in Austin, Texas on November 5, 2015. The FTC has announced that this workshop will be aimed at start-ups and developers and will include panels on such topics as creating a culture of security, adapting security testing for a high-growth environment, managing risks from third-party code and services, and overcoming development challenges to adopt security features that could impact performance.

SEC Issues Cybersecurity Risk Alert

On September 15, 2015, the Office of Compliance Inspections and Examinations ("OCIE") of the Securities and Exchange Commission ("SEC") issued a risk alert to provide information on the areas of focus for the OCIE's second round of cybersecurity examinations. The alert identifies six areas of focus for these examinations: (1) Governance and Risk Assessment; (2) Access Rights and Controls; (3) Data Loss Prevention; (4) Vendor Management; (5) Training; and (6) Incident Response.

The alert states that examiners may assess whether firms are periodically evaluating their cybersecurity risks and whether senior management and the board of directors are appropriately involved in the firm's cybersecurity risk assessment process. The alert also states that firms should implement basic access controls, such as multifactor authentication and updating access rights immediately following personnel changes. Examiners may also seek to determine what measures a firm is taking to monitor for potentially unauthorized data transfers. Additionally, examiners will seek to determine if firms have robust vendor management programs involving performing due diligence when selecting vendors, including contract terms pertaining to security, and monitoring and oversight of vendors. Finally, the alert states that examiners will determine whether firms have implemented an incident response plan and appropriate training to properly execute the plan in the event of a breach. The alert also includes a sample list of information that examiners may request when reviewing cybersecurity matters.

DoD Imposes Breach Reporting Obligations on Contractors and Subcontractors

On August 26, 2015, the Department of Defense ("DoD") issued an interim rule on Network Penetration and Contracting For Cloud Services that requires any DoD contractor or subcontractor to safeguard unclassified Covered Defense Information ("CDI") and report cyber incidents within 72 hours.[1] CDI is defined as unclassified information falling into one of four categories: (i) technical information, (ii) critical information related to operations security, (iii) export control information, or (iv) other restricted information identified by the contract itself. Contractors must apply security controls prescribed by the National Institute of Standards and Technology (NIST) to ensure safeguarding under contract requirements, or obtain a written waiver from the DoD Chief Information Officer.

The rules define a cyber-incident as any event compromising or having an actual or potentially adverse effect on a system or the information residing therein. After reporting a cyber-incident within 72 hours, a contractor must isolate any malicious software, maintain system images for 90 days to allow for DoD forensic analysis, and mark any trade secrets or commercially sensitive information ("Attributional Information") to safeguard against public release. The rule also obligates DoD support contractors assisting in cyber incident response to protect against releasing "Contractor Attributional/Proprietary Information," which it defines as information that "identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company."

The DoD rule also covers cloud computing service contractors. Cloud services contractors must implement security controls under the Cloud Computing Security Requirements Guide. Contractors must maintain within the U.S. or outlying areas all government data not located on DoD premises, and must apply restrictions on access to, use of, and any disclosure of government data. The rule also governs "spillage," which requires a report if controlled information is transferred to an information system that is not accredited to a security level appropriate for the information (i.e., classified information transferred to an unclassified system, or controlled technical information transferred to a public drive). As with other DoD contractors, the rule requires cloud services providers and their subcontractors to report all cyber incidents, and similarly isolate malicious software, maintain system images for 90 days, and allow for DoD forensic analysis.

Article contributed by Government Contracts Partner Keir Bancroft.

NTIA Convenes Multistakeholder Process on Cybersecurity Vulnerability Research Disclosure

On September 29, 2015, the National Telecommunications and Information Administration ("NTIA") convened its first multistakeholder meeting on developing best practices or guidelines for cybersecurity vulnerability research disclosure. The meeting included representatives from technology companies, automobile manufacturers, academia, and security service providers who discussed various perspectives and goals of industry stakeholders as well as the challenges raised by emerging technology areas, such as connected devices.

There was consensus among the group that existing initiatives, including the issuance of security standards by the International Organization for Standardization, have not bolstered sufficient collaboration among vendors, researchers, and users to address cybersecurity vulnerabilities. In discussing solutions to enhance coordination among stakeholders, researchers emphasized an approach that would encourage technology companies to clarify the legal actions they would take against researchers that disclose the company's cybersecurity vulnerabilities. An alternative solution focused on the establishment of incentives to encourage vendors to fix cybersecurity vulnerabilities identified by researchers. Panelists explored whether vendors' existing intellectual property rights dissuade researchers from disclosing cybersecurity vulnerabilities that they identify in a company's software or IP address.

---

[1] Network Penetration Reporting and Contracting for Cloud Services, 80 Fed. Reg. 51739 (Aug. 26, 2015).

The group also discussed a possible standard vulnerability coordination maturity model, the elements of which were presented as: organizational (*e.g.*, executive support for responding to vulnerability reports); engineering (*e.g.*, documentation of trade-offs); communications (*e.g.*, receiving vulnerability reports); analytics (*e.g.*, aggregation of raw data to improve code quality); and incentives (*e.g.*, reward researchers for reporting bugs). With regard to emerging technology, the group agreed that potential public safety concerns surrounding possible cyber threats to connected cars and medical devices warrant special consideration in the development of best practices or guidelines. The date and location of the second meeting have not yet been set, but it is expected to take place in November.

NIST Releases Draft Framework for Cyber Physical Systems

On September 18, 2015, the National Institute of Standards and Technology ("NIST") released a draft framework ("Framework") for cyber physical systems ("CPS"),[2] a term that includes the "Internet of Things." The Framework was developed by the CPS Public Working Group ("Working Group"), which is comprised of representatives from industry, academia, and the government. The Framework outlines common definitions and vocabulary intended to assist CPS developers in addressing various concerns and interests involved in the development of CPS, such as smart buildings, smart phones, and self-driving cars.

The Framework sets forth common characteristics among CPS devices and systems to enhance interaction among smart platforms in the broader interconnected environment. NIST cites as an example of a common characteristic "the tight integration of physical and computing devices—such as movement sensors that inform your fitness bracelet how far you have walked…"[3] The Framework is divided into three components: domains (*i.e.*, the environments in which CPS operate), facets (*i.e.*, common activities involved in CPS development), and aspects (*i.e.*, common concerns associated with the development process). NIST is expected to release a second draft of the Framework following the initial public comment stage, which is open through Monday, November 2, 2015.

HHS Inspector General Calls for Stronger Oversight and Enforcement of HIPAA Privacy Standards

The Office of the Inspector General ("IG") at the Department of Health and Human Services issued two reports in September relating to data privacy and data security, with the first calling on the Department's Office of Civil Rights ("OCR") to strengthen its oversight of covered entities' compliance with privacy regulations, and the second calling on OCR to strengthen its follow-up of reported breaches of patient health information.[4] The reports were prompted by the rise of data breaches at covered entities, such as doctors, pharmacies, and health insurance companies. For the reports, the IG surveyed a statistical sample of privacy breach related cases investigated by OCR, including both large and small breach incidents, from September 23, 2009 to March 31, 2011 and interviewed various OCR staff members and officials.

As part of its review, the IG discovered that 27 percent of surveyed covered entities did not meet their Health Insurance Portability and Accountability Act ("HIPAA") safeguard requirements, and that health information was not being adequately protected. In an effort to improve OCR oversight of data security, the IG called for the full implementation of a proactive audit program to identify possible noncompliance with the HIPAA. This proactive audit program was required by the HITECH Act amendments to HIPAA, effective February 2010, but has not been completed to date. The lack of a proactive audit program led the IG to find that OCR's enforcement is primarily complaint driven, with half of studied cases finding at least one noncompliant standard at a covered entity. The IG called for the full implementation of a proactive audit program in order to allow OCR to monitor and discover HIPAA violations before complaints or breaches surface.

The IG reports also found that OCR has failed to appropriately follow up on breach events at covered entities. The reports found that the majority of closed cases found at least one violation of the HIPAA privacy rule, but that 23 percent of cases had incomplete documentation of what corrective actions were taken, or if remediation was complete. The reports also found that small breach information was not entered into OCR's tracking system, such that staff would be unable to determine if a covered entity had previously suffered a breach. The inability to track these small breaches over time caused OCR to have an incomplete view of a covered entity's compliance.

The IG offered several recommendations for OCR in order to address the reports' findings. First, the IG called for the full implementation of the proactive audit system, along with a searchable database to allow effective tracking of covered entities over time. This recommendation includes development of a searchable database of covered entities prior investigations and corrective actions in order to create a more comprehensive picture of that entity's compliance history, including all small breach incidents. Along with this searchable database, the IG recommended a requirement that

---

[2] National Institute of Standards and Technology, Draft Framework for Cyber-Physical Systems (Sep. 18, 2015), http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf.

[3] National Institute of Standards and Technology, NIST Releases Draft Framework to Help Cyber Physical Systems Developers (Sep. 18, 2015), http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm.

[4] Office of Inspector General, Dep't of Health and Human Serv., OCR Should Strengthen Its Oversight of Breaches of Patient Health Information Reported by Covered Entities (2015); Office of Inspector General, Dep't of Health and Human Serv., OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities (2015).

OCR staff check a covered entity's prior investigatory status during a new investigation. The report stated that this policy would allow OCR to take an entity's full compliance history into account when determining appropriate resolutions to investigations.

FCC Holds Workshop on Robocall Blocking

On September 16, 2015, the Federal Communications Commission ("Commission" or "FCC") held a workshop focusing on "robocall blocking" (the blocking of unwanted autodialed calls) and "caller ID spoofing" (a practice that involves altering caller identification with the intent to commit fraud). The workshop assembled telephone service providers, technologists, and other stakeholders to discuss potential policy and technology solutions that may reduce the incidence of unwanted autodialed calls, caller ID spoofing, and fraud.

In his opening remarks, FCC Chairman Tom Wheeler stated that the goal of the workshop was to establish meaningful benchmarks to enhance consumer protection associated with unwanted calls. He suggested that call blocking technology should be more readily available to consumers and made free of charge. The first panel addressed the need for call blocking services and currently available call-blocking services. Panelists noted a high volume of consumer complaints related to unwanted autodialed calls. Both state and federal government agency representatives discussed problems related to calls made from outside the United States.

The second and third panels focused on the call blocking services offered by third parties and carriers, including call-filtering and caller ID validation services. Panelists explained list creation, call authentication, and other technologies that are being developed by industry working groups. The final panel focused on identification and blocking of unwanted autodialed calls and calls with spoofed caller IDs before they enter the network. Panelists discussed the difficulties in tracing calls and advocated for information sharing.

In the States

California Governor Signs Bill Regulating Voice Recognition and Advertising for Connected Televisions

On October 6, 2015, Governor Jerry Brown of California signed A.B. 1116 into law. The bill amends the California Business and Professions Code to address the use of voice recognition in connected televisions, and the use or sale of voice recognition data and recordings for advertising purposes. Specifically, the bill defines a "connected television" as a video device designed for home use to receive television signals and reduce them on an integrated, physical screen display that exceeds 12 inches. However, it does not include a personal computer, portable device, or a separate device that connects to a television, including a set-top box, video game console, or digital video recorder.

The bill requires that the user, or a designated person installing the television, be presented with a prominent notice of a voice recognition feature during the initial set-up of a connected television. Additionally, any recordings collected through a voice recognition feature that were made to improve that feature shall not be sold or used for any advertising purposes. Manufacturers of connected televisions are liable only for functionality provided at the time of the original sale, and cannot be compelled to build specific features to allow law enforcement to monitor voice recognition features.

The bill does not contain a private right of action, but can be enforced through an action brought by the California Attorney General. A violation of the bill can result in an injunction, and a knowing violation may include a fine of up to $2,500 for each connected television sold or leased in violation of the bill. Consumers may not waive any right granted by the bill. The law takes effect January 1, 2016.

Marketplace

Ari Schwartz Joins Venable as Managing Director of Cybersecurity

Ari Schwartz, former Senior Director for Cybersecurity at the White House, joined Venable in October as the Managing Director of Cybersecurity Services. While at the White House, Mr. Schwartz played a critical role in developing and implementing the Obama Administration's cybersecurity and technology policy. He oversaw and coordinated all network defense cybersecurity policy, including critical infrastructure protection, federal network protection, supply-chain efforts, cybersecurity standards promotion, and information sharing.

In his new role, Mr. Schwartz will collaborate with litigators, former regulators, and legislative advisors to develop holistic strategies for addressing

cybersecurity concerns. Additionally, Mr. Schwartz will provide cybersecurity consulting services for the firm, and will help organizations to understand and develop risk management strategies. In doing so, Mr. Schwartz will rely upon the White House's Cybersecurity Framework as well as other planning tools to minimize risk.

International

EU Court Invalidates U.S. – EU Safe Harbor Framework

A series of developments in the month of October have impacted U.S. companies that collect or receive personal information from residents of the European Economic Area ("EEA"). On October 6th, the European Court of Justice ("ECJ") issued its long-anticipated opinion in the Schrems case, invalidating the 2000 European Commission "EC") decision which determined that the U.S.- European Union ("EU") Safe Harbor program was considered "adequate" under EU law, leading to the creation of the U.S.- EU Safe Harbor framework.[5] While the ECJ opinion had been anticipated after the court's Advocate General issued an advisory opinion to the same effect in late September, its immediate effectiveness has appeared to catch European Data Protection Authorities ("DPAs") off guard, leaving them searching for a response. The ECJ decision is self-executing and unable to be appealed.

The 15-year-old Safe Harbor framework was intended to reconcile differences in U.S. and European Union laws that generally prohibit the transfer of personal information from the EEA to jurisdictions such as the U.S. that were deemed to provide "inadequate" protections by EU standards. The over 4,000 U.S. companies who began self-certifying in 2000 to the Safe Harbor principles relied on the framework as a mechanism to facilitate transfers of personal information across the Atlantic.

Individual Member States have weighed in on both sides of the issue. The United Kingdom's Information Commissioner's Office ("UK ICO") issued a statement reflecting a measured tone—"The judgment means that businesses that use Safe Harbor will need to review how they ensure that data transferred to the US is transferred in line with the law. We recognize that it will take them some time for them to do this."[6] On the other side of the spectrum was the reaction of one German DPA, which issued an advisory statement interpreting the ECJ decision as not only questioning the validity of the Safe Harbor, but also some of the other mechanisms available for facilitating data transfer.

Attempting to coordinate a collective response is the Article 29 Working Group, an advisory group comprised of all of the DPAs. On October 18, it issued its first statement, which reaffirmed the validity of other data transfer tools during the period through January 2016 while the group considers the broader impact of the ECJ decision. Reflecting political compromise among the different Member States, the statement noted that DPAs may still exercise their powers in response to complaints, but also appeared to recognize that enforcement directed at companies for violations tied to the Safe Harbor framework that is not the result of complaints may be stayed.

On this side of the Atlantic, U.S. lawmakers on October 14th called on Secretary of Commerce Penny Pritzker and Federal Trade Commission Chairwoman Edith Ramirez to take action in light of the Safe Harbor ruling to include issuing guidance to the business community and to redouble efforts to conclude negotiations on a Safe Harbor 2.0. These negotiations, which have been ongoing since late 2013, do not yet have an end date in sight. Companies who have relied upon the Safe Harbor framework for transfers of consumer or human resources data from the EEA should be assessing their current practice and the feasibility of alternative data transfer mechanisms. Additional guidance from both U.S. and EU authorities should be forthcoming in the future weeks. In the meantime, expect continued developments from now until the end of January 2016.

European Commission Issues Clarification Regaring Data Retention Directive

On September 16, 2015, the European Commission ("Commission") issued a clarification regarding national data retention laws in the European Union ("EU").[7] The original EU Data Retention Directive was annulled by the European Court of Justice in April 2014, and in its clarification, the Commission emphasized that the decision of whether or not to introduce data retention laws is a purely a national decision.

The Commission stressed that it is not coming forward with any new initiatives on data retention, and that in the absence of EU rules, Member States are free to maintain their current data retention systems or set up new ones, so long as they comply with basic principles of EU law. The Commission stated that it is neither opposing, nor advocating for the introduction of national data retention laws. As part of its clarification, the Commission also

---

[5] *Maximilian Schrems v. Data Protection Commissioner*, C-362-14 (E.C.J. Oct. 6, 2015), http://curia.europa.eu/juris/documents.jsf?num=C-362/14.

[6] Press Release, Information Commissioner's Office, ICO Response to ECJ Ruling on Personal Data to US Safe Harbor (Oct. 6, 2015), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/.

[7] Press Release, European Commission, Statement on National Data Retention Laws, STATEMENT/15/5654 (Sept. 16, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm.

responded to reports claiming that it was planning to take action against the German draft data retention law. The Commission's statement denied such plans, noting also it is currently engaged in constructive discussions with German authorities regarding the legislation.

Canadian Telecommunications Authority Issues Enforcement Advisory Regarding E-Marketing

The Canadian Radio-television and Telecommunications Commission ("Commission") recently issued an enforcement advisory to businesses providing professional training services that are sending commercial electronic messages ("CEM") as part of their e-marketing practices. The advisory was issued in response to the Commission staff's observation that some services are sending CEMs to lists of emails gathered from public websites. The advisory is intended to provide direction and clarification in response to confusion over two forms of implied consent authorized under the law.

Existing law under Canada's Anti-Spam Legislation ("CASL") requires businesses to obtain either express or implied consent prior to sending CEMs. CASL places the burden of proving consent on the sender. Implied consent exists if: (a) the business or organization has an existing business relationship; (b) the business or organization has an existing non-business relationship, or (c) an email address is made publicly available on a website. The enforcement advisory, and related guidance published by the Commission, clarified the types of implied consent resulting from an existing business relationship and from conspicuous publication.

The guidance sets forth a series of elements to determine whether an existing business relationship exists, including the purchase of goods, the making of inquiries to the business, and the signing of a written contract. Regarding implied consent arising from conspicuous publication, the guidance states that the publication of email addresses must not be accompanied by a statement indicating that the persons do not want to receive CEMs at that address. In the absence of a statement, a business can send a CEM to the email address only if the message relates to the recipient's business role, functions, or duties in an official or business capacity. The guidance also recommends that professional training service businesses inspect their mailing lists to ensure compliance with CASL. When sending CEMs, businesses are advised to keep records and pay particular attention to whether they have established implied consent or obtained express consent, provided identification information, and included an unsubscribe mechanism.

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.

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