November 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

David L. Strickland

Ari M. Schwartz

Erik C. Jones

Julia Kernochan Tama

Kelly A. DeMarchis

Tara Sugiyama Potashnik

Matt H. MacKenzie

Rob Hartwell

Emma R. W. Blaser

Sheena R. Thomas

Chan D. Lieu

POLICY ANALYSTS:

Marissa L. Kibler

London M. Swift

Introduction

In this issue, we examine FTC related developments in data security, in particular the dismissal of the FTC's first data security complaint brought before an administrative law judge. On the privacy side, we review the FTC's workshop on cross-device linking as well as the FCC's denial of a "do not track" petition, among other federal agency activities. We recap several events on Capitol Hill, including the Senate's passage of cybersecurity legislation and a hearing on data brokers. Also discussed are international developments related to the U.S.-EU Safe Harbor and a series of bills enacted in California regarding data security.

In this Issue:

Heard on the Hill

House Hearings on Cross-Border Data Flows and Safe Harbor

On November 3, 2015, the U.S. House Energy and Commerce Committee's Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology held a joint hearing entitled "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows." On the same day, the U.S. House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet convened a hearing entitled "International Data Flows: Promoting Digital Trade In the 21st Century," which addressed similar issues.

During the Energy and Commerce joint Subcommittee hearing, Members and panelists discussed the importance of cross-border data flows; the close trade relationship between the United States and the EU; the EU court ruling on *Maximillian Schrems v. Data Protection Commissioner* ("*Schrems*") that invalidated the U.S.-EU Safe Harbor Agreement; and the renegotiation of the Safe Harbor Agreement. In her opening statement, Subcommittee Ranking Member Jan Schakowsky (D-IL) discussed her plans to introduce legislation regulating security standards for personal data, including geolocation, health, and biometric data, as well as email and social media account information. Subcommittee Chairman Walden (R-OR) and other Members focused on the ongoing Safe Harbor 2.0 negotiations in their questioning. Panelists commented that it is critical to reach an agreement before the January 31, 2016 deadline when EU data protection authorities will begin enforcing the *Schrems* decision, and suggested that the Department of Commerce's and the Federal Trade Commission's lack of authority over U.S. government surveillance may mean that Safe Harbor 2.0 will face future legal challenges in the EU.

In the Judiciary Committee hearing, Members emphasized the importance of the Safe Harbor agreement, and discussed potential legislative and policy solutions to the EU court's Safe Habor invalidation. Committee Ranking Member John Conyers (D-MI) highlighted the passage of the "Judicial Redress Act," noting that it was an important step in addressing Europeans' concerns regarding U.S. government surveillance. Subcommittee Chairman Darrell Issa (R-CA) and Subcommittee Vice Chairman Doug Collins (R-GA) discussed elements of the Trans-Pacific Partnership with the panel, including implications for banks and proposals that prevent countries from requiring companies to share source code or localize data centers.

Senate Judiciary Hearing on Data Brokers

On November 3, 2015, the Senate Judiciary Committee's Subcommittee on Privacy, Technology and the Law held a hearing entitled "Data Brokers – Is Consumers' Information Secure?" The panel consisted of witnesses from industry and the nonprofit sector, and focused on data security, consumer access and choice, sensitive data, and industry self-regulation.

Subcommittee Chairman Jeff Flake (R-AZ) noted the important role that data brokers play in the economy, such as offering complex risk mitigation and marketing services. Subcommittee Ranking Member Al Franken (D-MN) defined "data brokers" as companies in the business of collecting information about consumers in order to sell it to others for various purposes. He stated that Congress should do more to secure consumers' personal information, especially given the large amounts of data that certain companies maintain.

During the questioning period, Members discussed with panelists whether current federal data security standards needed to be updated and the need for a well-trained cybersecurity workforce. There was discussion about the extent to which consumers have knowledge of and are able to control the collection and use of data by data brokers. Regarding consumer control, the panel addressed online tools that allow consumers to opt out of certain data uses. The panel concluded with a discussion on the potential for industry self-regulation of data security, noting that industry can best assess the risks to the data it maintains and the appropriate level of security. The panel noted that federal data security legislation should set a "high bar" for industry if such legislation were to be considered.

Senate Commerce Hearing on "Non-Disparagement Clauses" Limiting Consumer Reviews

The Senate Committee on Commerce, Science, and Transportation held a hearing on November 4, 2015, entitled "Zero Stars: How Gagging Honest Reviews Harms Consumers and the Economy." Members and panelists discussed the use of "non-disparagement clauses" in form contracts to penalize consumers for negative reviews, with participants generally expressing concern about such clauses.

At the hearing, Chairman John Thune (R-SD) advocated for the Consumer Review Freedom Act ("CRFA") (S. 2044), a bill he authored to prohibit certain types of non-disparagement terms in form contracts, subject to enforcement by the Federal Trade Commission and state authorities. Ranking Member Bill Nelson (D-FL), a co-sponsor of the CRFA, voiced support in his opening statement for the Chairman's efforts. A companion bill, H.R. 2110, has been introduced in the House. Senator Richard Blumenthal (D-CT), although a co-sponsor of the CRFA, expressed support for removing limitations on state attorney general enforcement authority from the bill.

In addition to the CRFA, questioners and witnesses discussed related topics, including whether consumers are aware of non-disparagement terms in form contracts, how businesses should address negative or false reviews from consumers, and the provisions of the CRFA.

Senate Passes Cybersecurity Information Sharing Act

On October 27, 2015, the U.S. Senate passed the Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015), by a 74-21 vote.[1] The bill, sponsored by Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Dianne Feinstein (D-CA), would codify certain mechanisms for voluntary cybersecurity information sharing among private entities and the federal government. The bill also would provide liability protections to entities that monitor information systems or share or receive cyber-threat indicators or defense measures, provided that it is done consistently with procedures and exceptions set forth by the Department of Homeland Security.

CISA would require the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Department of Justice to establish procedures to encourage the following: (1) timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments; (2) the sharing of unclassified indicators with the public; and (3) the sharing of cybersecurity threats with entities to prevent or mitigate adverse effects.

Members of Congress are now considering whether, and how, to reconcile S. 754 with a House cybersecurity bill, H.R. 1560. The House bill, in turn, combines two cybersecurity measures passed in April entitled the "Protecting Cyber Networks Act"[2] and the "National Cybersecurity Protection Advancement Act of 2015."[3] Unlike the House bill, S. 754 would not provide immunity against "good faith" inaction on sharing of cyber threat indicators and defensive measures and applies only to the sharing and receipt of authorized cyber threat information.[4]

On privacy, S. 754 would require private entities to remove any personal information unrelated to a threat prior to sharing, whereas the House bill would require private entities to take "reasonable efforts" to remove personally identifiable information that is "reasonably believed" to be unrelated to a cyber-threat.[5] S. 754 would limit government use of information for law enforcement purposes involving imminent threats and does not address direct sharing with the National Security Agency ("NSA"). The House bill would not provide for sharing with the NSA and other surveillance authorities. Details regarding House-Senate conference negotiations to finalize S. 754 have not been announced, but it is expected that a conference committee consisting of Members of both parties, chambers, and all relevant committees will be appointed.

House Passes Judicial Redress Act

On October 20, 2015, the U.S. House of Representatives ("House") passed the "Judicial Redress Act," or H.R. 1428.[6] The stated purpose of the bill is to extend privacy rights and civil remedies of U.S. citizens set forth under the Privacy Act of 1974 ("Privacy Act") to citizens of certain foreign countries, including European Union ("EU") Member States. The bill would grant citizens of the specified countries the right to sue certain U.S. government agencies in U.S. courts for unlawful disclosure of these citizens' records held by these agencies, and to access or correct these records.

The bill applies to records of citizens of specified countries that contain information shared by covered countries with U.S. law enforcement for purposes associated with investigation, detection, and prosecution of criminal offenses. The bill, sponsored by Representative Jim Sensenbrenner (R-WI), has been referred to the Senate Committee on the Judiciary for consideration.

By extending judicial redress provided to U.S. citizens to EU citizens, the Act would help bring into force the U.S.-EU Umbrella Agreement ("Umbrella Agreement"). The Umbrella Agreement would establish a data protection framework for cooperation between the EU and United States with regard to law enforcement. The bill has been discussed by Members of Congress and industry stakeholders during two separate House subcommittee hearings on cross-border data flows held on November 3, 2015 as part of a potential solution to address the October 6, 2015 invalidation of the U.S.-EU Safe Harbor Framework.

[1] Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015).

[2] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015).

[3] National Cybersecurity Protection Advancement Act, H.R. 1731, 114th Cong. (2015).

[4] Protecting Cyber Networks Act, National Cybersecurity Protection Advancement Act, H.R. 1560, 114th Cong. (2015).

[5] Id.

[6] Judicial Redress Act, H.R. 1428, 114th Cong. (2015).

Around the Agencies

Administrative Law Judge Dismisses FTC Data Security Complaint Against LabMD

In the first of 55 data security enforcement cases ever brought by the Federal Trade Commission ("FTC" of "Commission") before an administrative law judge ("ALJ"), Chief ALJ D. Michael Chappell dismissed the FTC's claim that medical testing laboratory LabMD, Inc.'s alleged failure to institute reasonable data security standards constituted an unfair business practice under Section 5 of the FTC Act. The FTC's case against LabMD is one of only two not to have settled, with the other case currently pending in federal court.

In his initial decision issued on November 13, 2015, Judge Chappell dismissed the FTC's complaint based on the Commission's failure to prove by a preponderance of the evidence that LabMD's alleged conduct caused or is likely to cause substantial injury to consumers as required by the test for unfairness under Section 5(n) of the FTC Act. The complaint, which was filed on August 28, 2013 by the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection ("Complaint Counsel"), alleged that LabMD failed to properly maintain the security of its data, identify foreseeable security risks, or adequately train employees to protect personal information, among other allegations.[7] The FTC's Complaint Counsel has since filed an appeal with the FTC Commissioners, who are charged with reviewing the Chief ALJ's decision.

The initial decision cites three reasons in support of dismissal. First, the ALJ found that Complaint Counsel had not alleged a substantial injury to consumers, which is required for the FTC to have authority to enforce a complaint.[8] Second, the decision states that the FTC failed to prove that LabMD's alleged failure to reasonably secure data on its computer network caused, or is likely to cause, harm to consumers. Third, the ALJ found that the evidence fails to assess the degree of the alleged risk, or otherwise demonstrate the probability that a data breach will occur.

The FTC's complaint alleged that a 1,718-page insurance report ("1718 file") was available on a peer-to-peer sharing network, and Complaint Counsel relied on the opinions of experts to quantify the harm they alleged could occur as a result of exposure of the 1718 file. However, the ALJ found these experts to be unpersuasive, as Complaint Counsel could not identify a single instance of actual harm to any consumer whose information was exposed. Although the information was downloadable from the peer-to-peer network, it was not downloaded by anyone outside of the case, and therefore the ALJ found that the risk of substantial injury was low.

Furthermore, although the 1718 file contained some information about testing for "sensitive" health conditions, such as cancer and HIV, the ALJ found that potential embarrassment was not a substantial injury for two reasons: 1) the information was coded, and thus the sensitivity of it was not immediately discernable by anyone who downloaded the file; and 2) "subjective feelings such as embarrassment, upset, or stigma, standing alone, do not constitute 'substantial injury' within the meaning of Section 5(n)."[9]

Complaint Counsel also focused on allegations that LabMD failed to reasonably secure its data. A police investigation into suspected utility billing theft in Sacramento, California led to the discovery of LabMD paper documents containing personal information ("The Sacramento Documents"). The Sacramento Documents spurred the FTC's claim that LabMD's failure to reasonably secure data on its computer network caused, or is likely to cause, harm to consumers.

The ALJ rejected this claim, noting that FTC failed to prove that the documents were maintained on LabMD's computer network or explain how the documents were exposed. Moreover, the evidence failed to prove that the exposure of the LabMD documents caused, or is likely to cause, any consumer injury, and it was noted that the FTC was unable to identify any consumer who had suffered identity theft or identity fraud. According to the initial decision, the FTC was unable to confirm anything more than "the possibility of future harm, or an unquantified, inchoate 'risk' of future harm,"[10] and as a matter of law the possibility of harm cannot be equated with likelihood of harm.[11]

The initial decision also rejects the FTC's theory that harm is likely for all consumers with personal information on LabMD's computer network. This theory was based on the "risk" of a future data breach and resulting identity theft injury rather than a genuine breach. The ALJ expressed concern that allowing unfairness liability to be based on a risk of harm alone would expose any security system that fell short of perfection, and would make the "likelihood" of harm requirement in Section 5(n) of the FTC Act redundant.

[7] LabMD, Inc., Docket No. 9357, 1 (Nov. 13, 2015) (initial decision) [hereinafter Decision].

[8] Decision at 13.

[9] *Id.* at 68-69.

[10] *Id.* at 75.

[11] *Id.* at 87.

FTC Holds Lead Generation Workshop

On October 30, 2015, the Federal Trade Commission ("FTC") held a workshop entitled "Follow the Lead: An FTC Workshop on Lead Generation." Lead generation was defined as the creation of consumer interest in a product or service, and the distribution of that information to third parties. The workshop convened a variety of stakeholders, including industry representatives, consumer advocates, and government regulators. Panelists discussed the benefits and risks that accompany lead generation, and explained best practices and codes of conduct that can make lead generation more transparent.

The Director of the FTC's Bureau of Consumer Protection, Jessica Rich, began the workshop by emphasizing the economic value of lead generation. She contrasted lead generation's economic potential with its capacity for facilitating fraudulent activity. Ms. Rich asserted that the FTC's objective in this space is to ensure a fair and efficient marketplace for businesses and consumers.

Panelists conferred on how lead generation is used in the lending and education contexts, the intersection between lead generation and consumer protection, and the steps that both industry members and regulators can take to better protect and educate consumers. Assistant Attorney General for the State of Connecticut, Joseph J. Chambers, stated that attorney general offices need to develop a multi-pronged approach and technical expertise to address developments in the lead generation industry.

The acting Associate Director of the FTC's Division of Financial Practices, Malini Mithal, gave the closing remarks. She encouraged interested parties to submit comments on the lead generation industry to the FTC by December 20, 2015.

FTC Convenes Start with Security Conference in Texas

On November 5, 2015, the Federal Trade Commission ("FTC") convened a workshop in Austin, Texas entitled "Start with Security." The workshop was the second event held by the FTC focusing on providing startup businesses with practical resources and strategies to implement effective data security measures. FTC Commissioner Terrell McSweeny opened the workshop by advising companies that market the privacy and security features of their products that they must live up to their claims. She also encouraged companies to address well-known vulnerabilities and integrate best practices throughout the product development and design processes.

The workshop included presentations from four panels. The first panel discussed how startups can build a culture of security. The panelists discussed the importance of limiting data collection from consumers and encouraged companies to provide better information security training for their employees. They also recommended that companies implement a risk management framework to provide employees with a clear reporting path for potential security vulnerabilities. The second panel addressed methods to test security and identify vulnerabilities in the high-growth startup environment. One panelist suggested that security professionals should send security alerts only when necessary. The panelist further suggested that such alerts should provide clear, concise information about the vulnerability and should use language that is accessible to non-security personnel when presenting solutions. Another panelist recommended that startups automate routine security assessments and deploy continuous testing technologies.

The third panel of the workshop focused on the potential security risks of using third-party codes or services. One panelist recommended that companies using third-party service providers include security requirements in their contracts with vendors to ensure that these vendors are accountable for addressing future security vulnerabilities. Another panelist encouraged companies to adopt a "vulnerability coordinate maturity model" and to seek guidance from proven industry standards. Finally, in the fourth panel, panelists discussed the use of website encryption and multifactor authentication. Panelists encouraged startups to adopt these tools and noted that their use does not significantly limit a website's performance. The FTC will hold its third "Start with Security" workshop on February 9, 2016 in Seattle, Washington. The workshop will focus on the measures small companies can take to secure their applications and products.

FTC Holds Workshop on Cross-Device Linking

On November 16, 2015, the Federal Trade Commission ("FTC") held a workshop in Washington D.C. titled "Cross-Device Tracking: An FTC Workshop." The workshop focused on the technology behind cross-device linking, as well as emerging policy initiatives around the issue. Chairwoman Edith Ramirez opened the event, after which two panels discussed technological advances, consumer benefits, potential privacy and data security risks, and the role of industry self-regulatory programs as they relate to cross-device linking.

Chairwoman Ramirez opened the workshop by highlighting various consumer benefits to cross-device linking, including customized user experiences and security and fraud prevention. She also noted that the rise in wearable and mobile technology has allowed companies to leverage several data streams to create more robust consumer profiles. She discussed various challenges presented by cross-device linking, such as transparency and control related to consumer privacy, and

advocated for data minimization and enhanced data security. The FTC praised the Digital Advertising Alliance's ("DAA") recent guidance on how its self-regulatory principles apply to cross-device linking, and warned that the FTC will continue to monitor for deceptive and unfair practices in the space.[12]

After a brief presentation of an overview of cross-device linking, the panels first discussed the technological process for linking and then the policy ramifications of the technique. The technology panel focused on how companies may associate devices with a consumer, either through "deterministic" techniques involving login credentials or "probabilistic" techniques based on inferences made from device information like IP address and browsing behavior. The panel also discussed ways that companies could protect consumer information, such as hashing, and how the industry has developed self-regulatory principles to place certain restrictions on data retention.

The policy panel focused on broader policy issues raised by cross-device linking. Genie Barton of the Council of Better Business Bureaus, which administers one of the DAA's Accountability Programs, noted that the DAA's Principles provide consumers with meaningful notice and control related to data collection and use. She continued to highlight that the DAA's self-regulatory approach produced guidance that provides for transparency and control related to cross-device linking. Other panel members stated that consumer education around cross-device practices is needed, and that consumers want to understand what happens to data about their devices. Ms. Barton noted that when consumers learn about interest-based advertising, and their ability to opt out of such practices, consumers tend to choose to continue to participate.

FCC Denies Consumer Group's "Do Not Track" Petition

On November 6, 2015, the Federal Communications Commission ("FCC") denied a petition filed in June 2015 that requested that the FCC regulate "edge providers" as part of its net neutrality rules implementing Section 222 of the Communications Act.[13] Edge providers are companies that offer content, apps, and services online to consumers, and the petition sought to require those companies to honor "Do Not Track" requests from consumers' Internet browsers. In its order denying the petition, the FCC ruled that the petition's request was "inconsistent with the Commission's articulation of the effect of its reclassification."[14]

The FCC adopted its "Open Internet Order" on February 26, 2015, reclassifying broadband internet service providers as common carriers, subject to the various regulatory and privacy requirements of the Communications Act.[15] Section 222 relates to the privacy of customer information, and restricts how covered entities may use customer data. The existing rules set out specific use limitations and data protection requirements for how common carriers manage their Customer Proprietary Network Information.[16] The petition asked that any new rules the FCC issued as a result of that order should expand the scope of data and companies governed by the rule. However, the FCC's Open Internet Order specifically stated that it was not "regulating the Internet, *per se*, or any Internet applications or content." Accordingly, the FCC denied the petition.

In the States

California Governor Signs Data Security Bills and CalECPA

On October 6, 2015, California Governor Jerry Brown signed three bills amending California's breach notification statute. The first bill, A.B. 964, adds a definition for the word "encrypted" in California's breach notification statute. The Act defines "encrypted" as data that is "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." The second bill, S.B. 570, adds content requirements for the notices that must be sent to consumers following a data breach. Specifically, it requires that the notices be titled "Notice of Data Breach" and contain the following sections: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." The bill also includes a model breach notification form. The third bill, S.B. 34, provides that information collected using an automated license plate recognition system constitutes personal information for the purposes of California's breach notification statute when such information is not encrypted and is used in combination with an

---

[12] DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (2015) *available at* http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf.

[13] 47 U.S.C. § 222.

[14] Petition for Rulemaking to Require Edge Providers to Honor "Do Not Track" Requests, Order, DA 15-1266, RM-11757 (Nov. 6, 2015) at 2, *available at* https://www.fcc.gov/document/bureau-dismisses-petition-regulate-edge-provider-privacy-practices.

[15] *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).

[16] 47 C.F.R. §§ 64.2001 *et seq.*

individual's name. The bill further provides that automated license plate recognition operators and end-users must implement security procedures and practices as well as privacy policies. The new laws take effect on January 1, 2016.

On October 8, 2015, Governor Brown also signed the California Electronic Communications Privacy Act, S.B. 178. The new law requires a search warrant, or other judicial authorization, for law enforcement to require a service provider to produce or provide access to an individual's electronic communication information or electronic device information. The Act defines "electronic communication information" to include both the content of a communication and its metadata. It further defines "electronic device information" to include any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device. The Act does not prevent state law enforcement from requiring the originator or intended recipient of an electronic communication to disclose any electronic communication information. It also does not prevent state law enforcement agencies from requiring an entity that provides electronic communication services to employees for work purposes to disclose electronic communication information, nor does it prohibit law enforcement from using a subpoena to obtain subscriber information from a service provider. The new law becomes effective on January 1, 2016.

International

U.S.–EU Safe Harbor Update

Following the announcement of the European Court of Justice ("ECJ") decision on October 6, 2015 invalidating the U.S.-EU Safe Harbor ("Safe Harbor"), U.S. government stakeholders continue to urge action, starting with Department of Commerce Secretary Penny Pritzker. In recent remarks at the AmCham Germany Annual Transatlantic Business Conference in Frankfurt, Secretary Pritzker asserted that the Safe Harbor issue is an "urgent problem." She noted that the improved Safe Harbor Framework that the U.S. has negotiated with the European Commission ("EC") over the past two years is the sensible solution. In addition, on November 3, 2015, the U.S. House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology held a joint hearing to draw congressional attention to the impact of the Safe Harbor decision. Members of the subcommittees and panelists discussed the economic impact of cross-border data flows, the trade relationship between the United States and the EU, and the legal challenges of renegotiating the U.S.-EU Safe Harbor Agreement.

On November 6, 2015, the EC issued its long-awaited guidance describing how companies should address compliance challenges in the immediate interim of the ECJ decision.[17] The guidance provided an overview of alternative tools for transatlantic data transfer. Specifically, the guidance addressed the implementation of model contract clauses and binding corporate rules. Additionally, the guidance outlined alternative "derogations" to the 1995 Directive that provide exceptions from the general prohibition against data transfers without an adequacy determination. The guidance noted that the burden to comply with the directive is on the data controllers. Moreover, EU data protection authorities will maintain the power to investigate individual cases. The EC guidance concluded by stating that a new Safe Harbor Framework is a key priority. The EC has "intensified" talks with the U.S. government, and the Commission plans to conclude negotiations within three months.

In other updates from the EU, German authorities issued a position paper stating that they will not approve any new transfers of data to the United States. The German ban on data transfers includes transfers based on alternative arrangements, such as those outlined in the EC guidance.

FTC and Seven International Partners Launch New Initiative to Boost Cooperation in Protecting Consumer Privacy

On October 25, 2015, Federal Trade Commission ("FTC") Chairwoman Edith Ramirez signed a Memorandum of Understanding ("MOU") with the seven other members of the Global Privacy Enforcement Network ("GPEN") to create a new system called "GPEN Alert."[18] GPEN Alert will allow participants to share information about investigations in a confidential and secure manner. The United Kingdom's Information Commissioner's Office—also a participant—explained that the agreement will allow members to share information while protecting it with appropriate safeguards. The seven other initial participants in GPEN Alert are the privacy commissioners of: Australia, Canada, Ireland, the Netherlands, New Zealand, and

[17] *Communication to the European Parliament on the Transfer of Personal Data from the EU to the United States of America,* COM (2015) 566 final (Nov. 6, 2015).
[18] Press Release, Fed. Trade Comm'n, FTC and Seven International Partners Launch New Initiative to Boost Cooperation in Protecting Consumer Privacy (Oct. 26, 2015), https://www.ftc.gov/news-events/press-releases/2015/10/ftc-seven-international-partners-launch-new-initiative-boost.

Norway. GPEN Alert is a response to the FTC's increasing need to coordinate with foreign regulators as U.S. companies conduct more business overseas.

GPEN Alert will use the same network operated by the FTC for its Consumer Sentinel Network ("CSN"), which allows information sharing among law enforcement agencies in the United States, but will be separate from the CSN. Only authorities that have signed a MOU and whose staff have security credentials will be permitted to access the system. At this time, the system does not allow law enforcement to share consumer complaints or confidential enforcement matters.

Israel Restricts U.S. Data Transfers in Light of Safe Harbor Decision

While the October 6, 2015 European Court of Justice (ECJ) decision invalidating the U.S.-EU Safe Harbor continues to have implications for transatlantic data transfer, the repercussions of the decision have now traveled to Israel. In late October, the Israeli Law, Information and Technology Authority (ILITA) revoked its prior authorization for data transfers from Israel to the United States based on the U.S.-EU Safe Harbor. Israel's privacy law, the Privacy Protection Regulations of 2001 (the "2001 Regulations"), largely followed EU law and prohibited the transfer of data from Israel to a location that did not ensure a level of protection equal to or greater than that required by Israeli law. In fact, Israel is one of the few countries recognized as having an "adequate" level of protection as defined by the EU Data Protection Directive.

The 2001 Regulations recognize certain permissible data transfers, including transfers to countries that receive information from Member States of the European Union and European Economic Area in accordance with the requirements under European data protection law. Prior to the ECJ ruling, Israel had recognized transfers to entities certified under the Safe Harbor as also meeting the requirements for lawful transfers under Israeli law. In light of the ECJ decision, the ILITA has revoked this prior authorization for data transfer. At present, ILITA has not publicly addressed whether other methods of data transfer recognized by EU Member States, such as model contracts, are valid under Israeli 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
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000

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

SAN FRANCISCO, CA
505 MONTGOMERY STREET
SUITE 1400
SAN FRANCISCO, CA 94111
t 415.653.3750

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

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

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