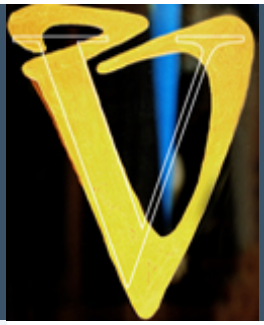
VENABLE LLP



the download

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

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

.....

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
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

Ariel S. Wolf
awolf@Venable.com
202.344.4464

November 2014

In this Issue:

.....

www.Venable.com

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Robert Hartwell
rhartwell@Venable.com
202.344.4663

Liz T. Oesterle
etoesterle@venable.com
202.344.4706

David L. Strickland
dlstrickland@venable.com
202.344.4747

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Matt H. MacKenzie
mhmckenzie@Venable.com
202.344.4754

Emma R. W. Blaser
erblaser@Venable.com
202.344.4225

Chan D. Lieu
cdlieu@venable.com
202.344.4842

Heard on the Hill

House Energy and Commerce Subcommittee Hearing on Data Flows

On September 17, 2014, the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") held a hearing entitled "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs." Subcommittee members and witnesses discussed the benefits of international cross border data flows for a variety of industries, as well as the risks of limiting such data flows. The participants also discussed several related topics, including the E.U.-U.S. Safe Harbor Framework negotiations and their relation to cross-border data flows and potential protectionist policies.

The panel generally agreed that cross-border data flows are a vital piece of the U.S. economy and that a restriction on that flow would represent a significant non-tariff trade barrier. It was stated that approximately 40 million American jobs are supported by industries that rely on intellectual property and data flows, and that those industries represent 60% of U.S. exports. Chairman Lee Terry (R-NE) suggested that a Congressional Resolution to the U.S. Trade Representative or Department of Commerce may be helpful in voicing the seriousness with which the U.S. takes the issue.

When discussing the cause of the recent proposals in some countries to limit data flows to the U.S., the panel noted recent revelations about government surveillance and retail consumer data breaches as two motivating factors. It was suggested that Congress should reassess the Foreign Intelligence Surveillance Act to address surveillance concerns, and that the U.S. should review its current framework of privacy laws for areas of improvement. Additionally, Ranking Member Jan Schakowsky (D-IL) voiced support for the USA FREEDOM Act, H.R. 3361, and the Data Accountability and Trust Act, H.R. 4400, as two pieces of legislation that could address some of those concerns.

Senate Judiciary Committee Hearing on Net Neutrality

On Wednesday, September 17, 2014 the Senate Committee on the Judiciary held a hearing entitled "Why Net Neutrality Matters: Protecting Consumers and Competition through Meaningful Open Internet Rules." Committee Chairman Senator Patrick Leahy (D-VT) presided over the hearing, which followed the conclusion of the Federal Communications Commission's ("FCC") comment period concerning proposed net neutrality rules.

The newly proposed rules seek to replace rules that were struck down by the D.C. Circuit Court of Appeals in January 2014. The

new proposal continues to rely on existing FCC authority and would not reclassify internet service providers as common carriers under Title II of the Communications Act. The proposed rules generated a record number of comments, with more than 3.7 million filings submitted to the FCC. The large amount of interest was on display at the hearing.

Both proponents and opponents of the net neutrality rules were present at the hearing. Echoing statements made by Senator Chuck Grassley (R-IA), one witness stated that the FCC should not regulate the Internet and that the current Internet access market does not need fixing. On the other side, Senator Al Franken (D-MN) stated that a lack of net neutrality would limit innovation and alter the status quo of the Internet ecosystem. FCC Chairman Tom Wheeler has stated that he hopes to conclude the rulemaking process on this issue by the end of the year.

ECPA Legislation Under Congressional Consideration

September featured several developments in the ongoing debate over the limits on the government's ability to access personal electronic communications.

- On September 9, 2014, a group of technology companies and advocacy groups sent a letter to Senate Majority Leader Harry Reid (D-NV) and House of Representatives Majority Leader Kevin McCarthy (R-CA) urging them to advance S. 607 and H.R. 1852, legislation that would amend the Electronic Communications Privacy Act (ECPA) to require that the government obtain a warrant to access the contents of electronic communications held by third-party service providers. The bills are opposed by executive agencies that have expressed concern about their ability to conduct investigations without the ability to obtain the content of documents and communications from internet service providers.[1] The letter called for certainty regarding the standards for government access to data stored online to maintain consumer trust in cloud computing services, and opposed a carve-out from the warrant requirement for regulatory agencies.

- On September 16, 2014, Senators Orrin Hatch (R-UT), Chris Coons (D-DE), and Dean Heller (R-NV) introduced the Law Enforcement Access to Data Stored Abroad Act ("LEADS" Act). The bill would require the government to obtain a search warrant to access the contents of electronic communications sent or received by U.S. citizens,

[1] *See* S. REP. NO. 113-34 at 17-18 (2013), *available at* https://www.congress.gov/113/crpt/srpt34/CRPT-113srpt34.pdf.

permanent resident aliens, or companies incorporated in the United States that are stored on servers located in another country. A warrant would be modified or vacated if a court determined that the warrant would require the service provider to violate the laws of another country. The bill follows a decision by a magistrate judge of the United States District Court of the Southern District of New York who refused to quash a warrant issued under the Stored Communications Act that required a software company to produce communications stored on a server located in Ireland.

From the White House

Updates on Recent Regulatory Activities Regarding Drones

Drones have been making news lately and the amount of recent regulatory attention to the issue reflects the rapidly changing landscape in which drones are operating. We summarize some recent initiatives in this area below.

- The White House is currently working on an Executive Order ("Order") that would regulate federal agency drone use. Specifically, it is reported that the Order would instruct the Department of Commerce to help develop voluntary privacy guidelines for private-sector drone flights, with the intent that these guidelines would help shape nonbinding industry standards on commercial surveillance. The Order would also increase transparency into drone use by the federal government, by directing federal agencies such as the Pentagon, Justice Department, and Department of Homeland Security to provide public information about the size and surveillance capabilities of their drone fleets operating in U.S. airspace. At present, the draft Order is in the interagency review process; no formal timetable has been set for its release.

- On September 30th, the Government Accountability Office published a report summarizing the Department of Homeland Security's ("DHS") review of the U.S. Customs and Border Protection's ("CBP") drone program for border surveillance.[2] The DHS review found that CBP had taken steps to help ensure that its drone program complied with privacy and civil liberty laws and standards. The review revealed that drones were sometimes flown away from the border "in support of other federal, state or local law enforcement activities and for emergency and

[2] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-849R, UNMANNED AERIAL SYSTEMS: DHS'S REVIEW OF U.S. CUSTOMS AND BORDER PROTECTION'S USE AND COMPLIANCE WITH PRIVACY AND CIVIL LIBERTY LAWS AND STANDARDS (2014), *available at* http://www.gao.gov/assets/670/666282.pdf.

humanitarian efforts," but that CPB uses an "oversight framework and procedures" to ensure compliance with all privacy laws. The Report also discussed a DHS "Working Group" tasked with establishing a forum for privacy issues; ensuring that DHS Privacy Office guidance was reflected in drone policies; identifying potential privacy and civil liberties concerns with drone use; and promoting best practices for safeguarding privacy, civil rights, and civil liberties by DHS partners. As part of these best efforts, the Privacy Office issued a privacy impact assessment in September 2013 finding that drone use as it was being conducted by DHS, was consistent with the Fair Information Practice Principles.

- On September 25th, the Federal Aviation Administration ("FAA") cleared six filmmaking companies to use drones for filming, marking the first exemptions on the FAA's virtual ban on commercial drone use. Although the FAA continues to work on rules for commercial drone use—a process expected to stretch into next year at a minimum—the FAA previously signaled its willingness to approve operating requests for commercial drones, especially those operating in controlled environments away from populated areas, for uses such as filmmaking, crop monitoring, and power plant inspections. The FAA is currently considering approximately 40 other requests for exemptions spanning a number of different commercial sectors, and has imposed a 120-day period on itself for review.

Around the Agencies

FTC Hosts Workshop on Big Data

On September 15, 2014, the Federal Trade Commission ("FTC") hosted a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" The workshop brought together a variety of speakers to discuss what steps, if any, need to be taken to promote the benefits that flow from the use of data analytics while protecting against the potential for this information to serve as a basis for discriminatory decisions.

Both Chairwoman Edith Ramirez and Commissioner Julie Brill spoke at the workshop. In addition to touting the benefits of big data and warning of its potential risks, Chairwoman Ramirez discussed the objectives for the FTC in this area, including enforcing existing laws and working with businesses to address alleged biases in predictive algorithms. Commissioner Brill called for privacy and fairness protections in big data analytics, emphasizing the importance of transparency and accountability

in maintaining consumer trust. She noted that regulatory attention would focus specifically on "alternative scoring practices," activities of "data brokers," companies' uses of customer data, and whether these practices could exacerbate existing socioeconomic disparities.

The panelists discussed the potential for big data analytics to bring low-income and underserved populations into the credit and employment markets. Some panelists cautioned that entities using big data analytics should consider the potential for discrimination when identifying data sources and drawing conclusions from the data they collect. Other panelists identified a number of examples in which organizations were able to include more people from underserved populations by identifying alternative factors to inform their decision through the use of big data. Specifically, some panelists discussed the use of data analytics to identify low-income individuals who lack a credit score because they do not frequently use credit products but nonetheless present a low risk of default.

Jessica Rich, the Director of the Bureau of Consumer Protection, concluded the workshop with an overview of the issues discussed during the workshop and the potential benefits and harms that could flow from the use of big data. She urged industry to use big data for positive benefits and to develop ways to avoid the harmful uses of big data. She also stated that the FTC will continue to investigate uses of big data that violate current laws and regulations.

CFPB Finalizes Rule Permitting Online Disclosure of Annual Privacy Notice

On October 20, 2014, the Consumer Financial Protection Bureau ("CFPB") finalized a new rule that will permit some financial institutions to deliver the annual privacy notice required by the Gramm-Leach-Bliley Act by publishing the notice on its website. The new rule applies only to financial institutions whose information sharing practices are such that the financial institution is not required to provide its customers with notice of their right to opt-out of certain information sharing. The new rule also requires that financial institutions use the model form provided in Regulation P and does not apply where a financial institution makes changes to its annual privacy notice that were not included in a previous notice to a customer.

The new rule also requires that a financial institution that chooses to rely on the online disclosure method must continuously post the annual privacy notice in a clear and conspicuous manner on a page of its website that does not require a login or agreement to any conditions to access. Further, the financial institution must provide consumers with an

annual reminder of the availability of the privacy notice. This reminder may be included on a regular consumer communication, such as a monthly billing statement or account statement. The reminder must inform customers that the annual privacy notice is available on the financial institution's website and that customers may call a phone number provided in the annual reminder to request that the financial institution mail a copy of the annual notice. Where a customer requests a mailed copy of the annual notice, the financial institution must mail the notice within ten days of the request.

FTC Publishes First COPPA Enforcement Actions Under Revised Regulation

The Federal Trade Commission (FTC) announced two settlements of enforcement actions involving the Children's Online Privacy Protection Act ("COPPA") on September 17, 2014. These settlements are the first COPPA cases the agency has made public since its revised COPPA regulation went into effect in July 2013. Although not focused on the aspects of the COPPA regulation that were revised, the cases reaffirm the agency's interest in enforcing COPPA against mobile apps.

One case was brought against Yelp, which offers a website and apps for consumers to post reviews of businesses. The FTC's complaint charges that Yelp apps accepted registrations from users who indicated that they were younger than 13, and thus acquired "actual knowledge" that these users were children. Allegedly, the Yelp app then collected from such registered users a variety of data that included "personal information" as defined by COPPA, without providing notice and obtaining verifiable parental consent as required by COPPA.

To settle the enforcement action, Yelp agreed to pay a $450,000 civil penalty, to comply with COPPA in the future, and to delete personal information previously collected from children within 30 days. In a blog post discussing the case, Lesley Fair of the FTC stated that the Yelp case "shows that COPPA isn't just for kids' sites" and encouraged companies to assess their mobile apps, including those provided by contractors, and to act on the information that users provide through an age screen.

The FTC's other case involved a company called TinyCo, which offers numerous game apps for mobile platforms. The FTC concluded that certain TinyCo apps are "directed to children" under the COPPA regulation, noting that the apps contained simple language; brightly animated characters; and subject matters including a zoo, tree house, and fairy tale references. The complaint against TinyCo alleged that the company had nevertheless failed to provide notice and obtain verifiable parental consent to collect email addresses from its users.

TinyCo agreed to pay a $300,000 civil penalty, to comply with COPPA going forward, and to delete all personal information collected by children within 10 days.

GAO Report on CFPB Big Data Collection

On September 22, 2014, the U.S. Government Accountability Office ("GAO") published a report on the Consumer Financial Protection Bureau's ("CFPB") collection of consumer financial data entitled, "Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced" ("Report"). The Report discussed the CFPB's adoption of privacy and data security policies and procedures to protect the financial consumer data it collects for use in its rulemakings, examinations, and reports (e.g., the Report states that the CFPB anonymizes large scale data collections). However, the Report also stated that many of these policies and procedures are not fully documented or implemented. To help improve the CFPB's data security efforts, the GAO issued recommendations for the CFPB, including:

Establishing or enhancing written procedures for:

1. Data intake;
2. Anonymizing data;
3. Evaluating privacy risks;
4. Auditing privacy controls; and
5. Documenting information security risk assessment results.

Implementing privacy and security steps, including:

1. Developing a comprehensive privacy policy and guidance plan;
2. Obtaining reviews of the CFPB's privacy practices;
3. Implementing privacy training;
4. Updating remedial plans for the information system to include identified weaknesses; and
5. Evaluating compliance with contract provisions of the CFPB's service provider that processes consumer financial data for the CFPB.

In the States

California Enacts Ten New Laws

Recent weeks have seen a flurry of legislative activity in California in the privacy space. On September 29, Governor Jerry

Brown signed into law two bills regarding student privacy. On September 30, he signed into law eight bills addressing privacy concerns related to invasion of privacy, distribution of unauthorized images, and data collection and security.

Student Privacy

SB 1177 prohibits the creation and distribution of "profiles" of minor students. Furthermore, it prohibits K-12 websites and applications from using information they gather to target advertisements at the K-12 audience. The law requires website or app operators to have policies in place to promote compliance. The enactment of AB 1584 allows schools to contract with third parties for the maintenance of student records, but requires those contracts to include certain provisions, including details of security measures and a clarification that the records belong to the school.

Invasion of Privacy

The newly enacted AB 1256 expands liability for "invasion of privacy" by clarifying the type of activity protected from unwarranted capturing of images or photographs, and also would establish zones of privacy around schools and medical facilities. AB 2306 expands the definition of "invasion of privacy" by eliminating the existing physical trespass requirement. The change would render illegal the use of drones and other electronic devices to capture images of individuals in their homes. AB 1356 amends current law to include surveillance as behavior that could establish stalking. Furthermore, this bill allows plaintiffs to plead "substantial emotional distress" as an alternative to the existing standard of "reasonable fear."

Distribution of Unauthorized Images

AB 2643 allows plaintiffs to file a civil suit for damages against a defendant who posted intimate photos or videos of the plaintiff without consent. Previously, defendants were only subject to a criminal action. SB 1255 expands the criminal prohibition on posting unauthorized intimate images to include images taken by the subject (also known as "selfies").

Data Collection and Dissemination

AB 928 requires state agencies to maintain and conspicuously post a privacy policy, and to include in such policies provisions that address the relevance and purpose of data collection and the prohibition on sharing data without consent. AB 1710 (discussed in September's issue of The Download) requires that companies that offer free identity theft protection to notify consumers whose personal information has been breached of

that offer, if the breach has exposed certain types of sensitive information. SB 828 prohibits the State of California from aiding the federal government in data collection that the state knows to be illegal or unconstitutional.

International

Article 29 Working Party Opinion on Internet of Things

On September 16, 2014, the European Union's Article 29 Working Party ("Working Party") released an opinion on recent developments involving the Internet of Things ("IoT"). The opinion provides data controllers (e.g., device manufacturers, application developers, social platforms) guidance on how to comply with the EU legal framework on privacy and data protection when collecting personal data from certain devices. Additionally, the Working Party opinion lists potential privacy and data security challenges for the IoT landscape. The opinion notes its potential application to data controllers outside of the EU that collect personal data from connected devices of data subjects within the EU.

The opinion lists potential privacy and data security concerns regarding IoT, including: (1) obtaining consent across connected devices and applications; (2) profiling of individuals through the collection of personal data from outside parties; and (3) capability of unauthorized parties to make inferences on a data subject's lifestyle, habits, preferences, or their activity while at home. The opinion suggests that a lack of adequate privacy and data protection measures of one unsophisticated connected device may weaken the safeguards of another device it is connected to, regardless of whether the latter device provides adequate consent and opt-out tools.

While the Working Party's opinion discusses potential privacy and security concerns involving IoT, it recognizes that IoT holds "significant prospects of growth for a great number of innovating and creative EU companies." The Working Party notes that it will continue to provide guidance on how to comply with EU privacy and data protection law in the IoT landscape as it evolves.

About Venable's Privacy and Data Security Team

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

About Venable

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

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

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

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

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

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

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

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

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

VENABLE® LLP