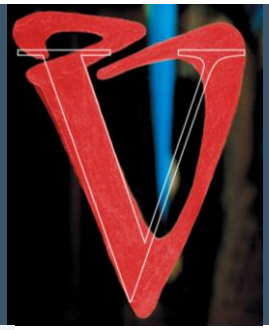
VENABLE LLP



the download

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

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

Ariel S. Wolf
awolf@Venable.com
202.344.4464

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Robert Hartwell
rhartwell@Venable.com
202.344.4663

www.Venable.com

September 2014

Welcome Back!

With Washington, DC emerging from its annual August recess, this issue recaps the summer's key privacy and data security developments in law and policy. For its part, Congress continued to examine data security issues while also beginning to explore the area of student privacy. Against the backdrop of a seminal Supreme Court case on law enforcement access to mobile phones, Congress also increased its focus on national security and government data collection.

The Administration and the agencies kept up the drumbeat on privacy issues. The FTC released new COPPA guidance, issued a report on mobile shopping apps, and announced a review of the Telemarketing Sales Rule. The White House hinted at a new regime for commercial drones, and NTIA continued its facial recognition multistakeholder process. The FDA released guidance on drug and medical device companies' use of Internet and social media platforms. It was also a busy season for state legislatures, as several states enacted new or updated breach notification laws, and one adopted a constitutional amendment on electronic privacy. In Europe, website operators brace for an impending enforcement sweep by data protection authorities.

In this Issue:

Around the Agencies

- FDA Social Media Guidance
- FTC Convenes September Workshop on Big Data
- FTC Studies Mobile Shopping Apps
- FTC Launches Review of Telemarketing Sales Rule
- FTC Expands COPPA FAQs Related to Verifiable Parental Consent

In the States

- Opposition to California Bill to Limit Capture of Personal Information During Online Credit Card Transactions
- Four States Enact New Data Breach Notification Laws
- Electronic Privacy Amendment Added to Missouri Constitution

International

- Euro "Cookie Sweep" Initiative
- UK Parliament Report Calls "Right to be Forgotten" Unworkable

.....

Heard on the Hill

House Committee Holds Hearing on FTC's Use of Section 5 Authority in Data Security Cases

On July 24, 2014, the House Oversight and Government Reform Committee (Committee) held a hearing entitled "The FTC and its Section 5 Authority: Prosecutor, Judge and Jury." Chairman Darrell Issa (R-CA) stated that he convened the hearing to consider whether the Federal Trade Commission (FTC) inappropriately targeted a company named LabMD and certain other companies for investigation after allegedly relying on possibly false information supplied by a security consultancy. Witnesses at the hearing—including the Chief Executive Officer of LabMD, a now-defunct medical testing company that has been subject to FTC enforcement—discussed the FTC's role in examining their companies' data security practices, and in particular, the FTC's ongoing administrative case against LabMD.

While the specifics of the LabMD case were discussed at the hearing and continue to be subject to ongoing Committee investigation, the overarching policy context of the hearing was the FTC's investigative and enforcement power in the area of data security. Lawmakers and witnesses focused on whether Section 5 of the FTC Act, which addresses "unfair or deceptive acts or practices," permits the agency to enforce data security standards, particularly in the absence of specific FTC guidance to industry on this topic.

On this point, one witness expressed concern that the FTC has not given guidance in the data security space that would allow regulated parties to be on notice of what practices may subject them to FTC enforcement, while another witness described the FTC's "reasonableness" standard. The Committee's examination of

data security enforcement comes at a time of increased attention from, and debate among, federal and state policymakers about data security legislation, as well as other significant cases addressing the limits of regulators' authority to set data security standards in the absence of express statutory authority.

Congress Considers Student Privacy; Department of Education Releases Guidance

A number of developments recently took place in the area of student privacy. On June 25, 2014, the House Education and the Workforce's Subcommittee on Early Childhood, Elementary, and Secondary Education (Education Subcommittee) and the House Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (Homeland Security Subcommittee) convened a joint hearing, entitled "How Data Mining Threatens Student Privacy." The hearing explored the implications of evolving and emerging technologies that foster the ability of instructors to use student data for individualizing and enhancing educational programs, and potential privacy concerns regarding the collection, use, and sharing of the student data that facilitates these advancements.

Members and witnesses discussed existing federal laws affecting student privacy, and whether such laws needed to be updated to account for emerging technologies and services. In particular, Members and witnesses addressed the Family Educational Rights Privacy Act (FERPA) of 1974, a law that gives parents certain rights with respect to children's student education records for schools that receive funding from the US Department of Education. A key issue raised in this context was FERPA's application to third parties. As was mentioned at the hearing, 95% of schools surveyed in a study were found to use third-party educational software and cloud services. It was noted that schools pursued these technologies and services for several reasons, including for data-driven educational goals, reporting obligations, cost savings, and instructional opportunities.

The hearing also addressed the trends associated with contracts between schools and vendors that handle student data. In this context, Members and witnesses addressed issues of data ownership, security, retention, destruction, breach notification, and use for marketing purposes.

On July 24, 2014, the US Department of Education's Privacy Technical Assistance Center (PTAC) released guidance entitled, "Transparency Best Practices for Schools and Districts," a document intended to provide recommendations for keeping parents and students informed about schools' and districts'

collection and use of student data.[1] Specifically, the guidance recommends that schools and districts:

- Make information about student data policies and practices easy to find on a public webpage;
- Publish a data inventory that details what information is collected about students, and what it is used for;
- Explain to parents what, if any, personal information is shared with third parties and for what purpose(s); and
- Use multi-layered communication strategies that tailor the complexity of the information to the medium, and inform parents where they can get more detailed information if they want it.

On July 30, 2014, Senators Ed Markey (D-MA) and Orrin Hatch (R-UT) introduced the Protecting Student Privacy Act, which would amend FERPA to prohibit programs administered by the US Department of Education from making funds available to any educational agency or institution that has not implemented information security policies specified in the law. These policies include the protection of personally identifiable information (PII) from education records, and the requirement that third parties to whom PII is disclosed have a comprehensive security program to protect such information. The bill was referred to the Senate Committee on Health, Education, Labor, and Pensions, where it awaits further action.

These efforts on student privacy follow the release of the Administration's "Big Data" report, which included a discussion about the collection and use of data in the educational context. The report, which was released on May 1, 2014, discussed the benefits of data applications and technological innovations, including new online course platforms that provide students real time feedback and personalized learning, while also calling on the federal government to ensure that educational data linked to individual students gathered in school is used for educational purposes, and not shared or used inappropriately.

National Security and Intelligence Gathering Efforts Move Ahead: NSA Surveillance Reform and Cyber Information Sharing

The month of July featured the introduction of two bills that continue efforts to reform government intelligence gathering and national security.

On July 10, 2014, the Senate Select Committee on Intelligence (Committee) approved a bill entitled the Cybersecurity Information Sharing Act of 2014 (S.2588 or CISA), co-authored by Chairman

[1] http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final.pdf.

Dianne Feinstein (D-CA) and Vice Chairman Saxby Chambliss (R-GA). The bill's authors stated that the purpose of the legislation is to encourage private and public sector entities to share information about cybersecurity and incidents with each other in order to identify and prevent cyber-attacks.

A critical feature of the legislation is language that provides liability protection to entities that share information in accordance with the processes and procedures set forth in the Act, and protects information shared with the government from disclosure. Critics have raised concerns that the bill encourages the private sector to share more information with the government. The introduction of CISA comes after the release of a discussion draft to federal agencies, private industry, and the public seeking comment. The bill has been placed on the Senate Legislative Calendar for further consideration by the full chamber.

On July 29, 2014, Senate Judiciary Committee Chairman Patrick Leahy (D-VT) and fourteen bipartisan cosponsors introduced the USA FREEDOM Act, (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act, or S. 2685). Like a previous version introduced in the Senate and a companion bill introduced in the House last October, the new Senate bill is intended to reform the National Security Agency's collection and storage of Americans' telephone records and Internet metadata under the USA PATRIOT Act (Pub. L. 107-56).

The new version of the USA FREEDOM Act was introduced in the Senate in response to concerns expressed by some legislators and stakeholders about changes made to the House bill prior to that bill's passage on May 22, 2014. The new version has been described by its authors as a compromise measure that has the support of the White House, the technology industry, and civil liberties groups, although the leadership of the Senate's Select Committee on Intelligence noted that the committee—which shares jurisdiction over the government's data collection program at issue—was not consulted in drafting the new language. The author of the House bill, Rep. Jim Sensenbrenner (R-WI), publicly expressed support for the Senate's new compromise language. It remains to be seen how, or if, the Senate will consider the USA FREEDOM Act in the brief period that remains for the 2014 legislative session.

From the White House

NTIA Privacy Multistakeholder Processes: Commercial Drones and Facial Recognition Technology

The White House confirmed that an inter-agency process is underway regarding the possible issuance of an executive order that would address privacy issues related to the operation of

commercial unmanned aircraft, or commercial drones. The executive order could include a directive to the National Telecommunications and Information Administration (NTIA) to facilitate a multistakeholder process for drafting a voluntary code of conduct for that would establish best practices for the commercial use of drones.

At the same time, the Federal Aviation Administration (FAA) has been working to meet a September 2015 deadline to issue rules that would allow for civil operation of small unmanned aircraft systems in US airspace. However, a June 26, 2014 report by the Office of Inspector General of the Department of Transportation found that the FAA is "significantly behind schedule" in meeting the goal of achieving safe integration by the September 2015 deadline, which was imposed by a statute enacted in 2012.

With a possible multistakeholder process on drones on the horizon, NTIA has continued to push ahead with the current process for facial recognition technology or FRT. On July 24, 2014, NTIA convened its ninth Privacy Multistakeholder Meeting for FRT, where participants continued to refine proposed definitions for the terms "facial detection," "facial categorization," and "facial identification." The group will focus on these terms as they move forward in crafting a voluntary framework. Other FRT issues that are expected to be discussed during the process are marketing, retention, destruction, and consumer choice. The next NTIA multistakeholder meeting on FRT is expected to take place in October.

Supreme Court Developments

Police Need Warrant to Search Arrestees' Mobile Phones (Riley v. California)

On June 24, 2014 the Supreme Court issued a ruling in *Riley v. California*[2] that requires police officers to obtain a warrant prior to searching the contents of a cell phone that was obtained during an arrest. The court was unanimous in its holding, with Chief Justice John Roberts writing for the majority and Justice Samuel Alito filing a concurring opinion. The opinion examined two fundamental questions: (1) was searching the contents of a phone required for officer safety or to preserve evidence; and (2) to what extent does a search of a cell phone intrude on a person's privacy.

On the first issue, Roberts noted that the digital data in a cell phone is incapable of being used as a weapon during an arrest. Therefore, while the Court acknowledged that an officer may examine the physical phone (*i.e.,* to check for hidden razor blades or other weapons) an officer does not have similar fears from data.

[2] *Riley v. California*, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

The Court also found that fears of evidence destruction were too remote, as the arrestee would presumably be restrained during the search.

When reviewing the level of protection the information on a phone should receive, Roberts noted that cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." The Court continued to discuss the myriad pieces of information that cell phones, especially smart phones, contain about our daily lives, noting that it is possible for the police to learn more about a person from their phone than even a search of their home may produce. Taking the two analyses together, the Court found that the police must obtain a warrant before searching a cell phone.

Justice Alito agreed in the result of the opinion, but filed a separate opinion to voice his concern that the case may have unintended consequences. He noted that under the Court's ruling, hard copy documents found incident to an arrest are properly obtained, but the same document on a phone is not. He suggested that legislatures may need to enact new laws with specific categories of information that should be protected from these types of searches, instead of relying on a blanket rule under the Fourth Amendment.

Around the Agencies

FDA Publishes Draft Social Media Guidance Documents

The Food and Drug Administration (FDA) has released drafts of two new guidance documents that are relevant to companies offering prescription drugs or medical devices (collectively, "medical products") using Internet and social media platforms. Such guidance expresses the agency's current views on the covered topics, but is not binding on companies or the FDA. Comments on both guidance documents are due by September 16, 2014.

First, the FDA issued Guidance on "Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices."[3] The draft emphasizes that companies are not required to monitor or respond to misinformation that is created or disseminated by independent third parties, including user-generated content that appears on a company's own social media forum. However, the guidance notes that companies may voluntarily choose to correct misinformation, and provides standards for doing so in a manner that will not trigger FDA objections. The draft guidance applies only where

[3] Food & Drug Administration, "Draft Guidance for Industry: Internet/Social Media Platforms – Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices" (June 2014), http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401079.pdf.

companies are not responsible for the initial misinformation. Among the principles set forth in the draft guidance, the FDA states that appropriate corrective information is relevant and responsive to the misinformation, limited and tailored to the misinformation, accurate, non-promotional, consistent with product labeling, and supported by sufficient evidence. A company need not respond to all misinformation that is posted, but should define what portion of a forum it is correcting and then address all misinformation within that portion.

The FDA also issued draft guidance on "Internet/Social Media Platforms with Character Space Limitations: Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices."[4] This draft guidance sets forth principles and hypothetical examples that are intended to help companies make required risk/benefit disclosures effectively using character-space-limited platforms. According to the FDA, where a specific platform does not allow for an accurate and balanced presentation of a product's risks and benefits, the company should reconsider using the platform for promotional messages.

FTC Convenes September Workshop on Big Data

The FTC has announced that it will hold a public workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" on September 15, 2014. This event follows the FTC's spring series of privacy workshops, which included an event focused on predictive analytics, and the release of the FTC's report on "data brokers" in early 2014.

According to the FTC's agenda, the workshop will consist of four panels on:

- The current uses of big data in a variety of contexts and how these uses impact consumers;
- Potential uses of big data as well as the potential benefits and harms for particular populations of consumers;
- Existing antidiscrimination and consumer protection laws and their application to big data activities; and
- Best practices for the use of big data to protect consumers.

The workshop also will feature remarks from FTC Commissioner Julie Brill and presentations from FTC staff. Pre-workshop comments were requested by August 15, but the FTC also will accept comments following the workshop until October 15.

[4] Food & Drug Administration, "Draft Guidance for Industry: Internet/Social Media Platforms with Character Space Limitations – Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices" (June 2014), http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401087.pdf.

FTC Studies Mobile Shopping Apps

Continuing its interest in the mobile apps environment, on August 1, 2014, the Federal Trade Commission ("FTC" or "Commission") released a new Staff Report on Mobile Shopping Apps, entitled, "What's the Deal? An FTC Study on Mobile Shopping Apps" ("Report").[5]

The Report made three key recommendations:

1. Apps should make clear consumers' rights and liability limits for unauthorized, fraudulent, or erroneous transactions.
2. Apps should more clearly describe how they collect, use, and share consumer data.
3. Companies should ensure that their data security promises translate into sound data security practices.

The Report studied the pre-download disclosures associated with 121 unique shopping apps, all of which were free to download. Apps were divided into three categories: (1) price comparison apps; (2) deal apps; and (3) in-store purchase apps.

Of these recommendations, the Report noted that many of the apps studied did not disclose whether dispute resolution or liability limits were offered prior to download. Although the apps studied did have privacy policies, the Report called the language in the policies "vague" which could make it difficult for consumers to understand how their data was potentially being collected, used, and shared. The Report also found that the vast majority of apps studied included language on data security, although the specifics of the promises were not verified.

The FTC has prepared a number of reports focused on mobile apps in recent years, including two reports on mobile apps for kids, a guide for mobile app developers on marketing mobile apps, and a staff report on mobile payments.

FTC Launches Review of Telemarketing Sales Rule

The Federal Trade Commission (FTC or Commission) launched a periodic review of the Telemarketing Sales Rule (TSR), for its effectiveness, costs, and benefits.[6] The Rule was previously amended in 2003, 2008, and 2010.

The Request for Comments solicits input on 38 questions (many of which contain multiple subparts), including whether there is a continuing need for all parts of the Rule or whether technology had

[5] The Report is available at http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf.
[6] The Request for Comment can be found at 79 F.R. 46732 (Aug. 11, 2014).

affected the Rule. The FTC seeks comment on specific questions regarding the TSR's recordkeeping requirements, the use of pre-acquired account information, and how negative option marketing transactions are treated. Other specific questions touch on self-regulatory efforts and the specific exemptions to the TSR, but all comments related to the Rule are welcome.

The original TSR was promulgated in 1995. The later amendments established the National Do Not Call Registry and addressed debt relief offers and prerecorded messages. The TSR applies generally to "telemarketing," which includes any "plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution…."[7] The Rule covers many different aspects of placing calls, billing for transactions conducted as a result of telemarketing, and using pre-acquired account information in connection with telemarketing transactions.

Note that the Request for Comment does not propose specific changes to the Rule at this time, although the comments could be used to help the FTC shape a future rulemaking proposal. Comments are due by October 14, 2014.

FTC Expands COPPA FAQs Related to Verifiable Parental Consent

Keeping with its promise to periodically revise and revisit its published guidance to the Children's Online Privacy Protection Act (COPPA) and its associated Rule, the Federal Trade Commission (FTC or Commission) expanded its guidance on verifiable parental consent methods acceptable under the Rule by providing two revised and one new FAQ on its webpage.[8]

While a list of acceptable verifiable parental consent mechanisms appears in the Rule, the Commission has always stated that the list is not exhaustive and that companies can implement other methods provided that they meet statutory standards of ensuring that a parent receives notice of information collection practices and authorizes the collection, use, and disclosure of their child's personal information. The new FAQs further clarify this point.

Updated FAQ H.5 confirmed the FTC's previously informal policy regarding use of a credit or debit card as a verifiable consent mechanism. Specifically, while FAQ H.5 does not change the FTC's longstanding position that entering a credit or debit card number *by itself* is not sufficient under the Rule, it also makes clear it is not necessary to charge the card. Instead, parents can be asked to supplement the request for credit card information, such as by asking parents to answer special questions that only the parents would know, or finding supplemental ways to contact the parent.

[7] 16 C.F.R. 310.2(dd).

[8] The complete list of COPPA FAQs is available here: http://business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

Updated FAQ H. 10 and new FAQ H. 16 discuss verifiable parental consent in a mobile app store environment. FAQ H. 10 makes clear that entry of a parent's app store password is not sufficient in and of itself to meet the standard for verifiable parental consent, but the app store account plus other indicia of reliability is sufficient. It also notes that the app developer can rely on the app store's provisioning of consent, provided the developer ensures that COPPA's requirements are being met. New FAQ H. 16 views the same issue from the app market's perspective. It now makes clear that platforms such as app markets do not become subject to COPPA simply by allowing child-directed apps (which may be covered) on their platform. However, the third-party app store should evaluate any potential liability under Sec. 5 of the FTC Act, as it could be a potentially deceptive practice to misrepresent the level of oversight provided over apps directed to children.

The COPPA FAQs also have started including "last revised" information at the top of the FAQs, to more easily track changes.

In the States

Opposition to California Bill to Limit Capture of Personal Information During Online Credit Card Transactions

In June, a bill that would amend California's Song-Beverly Credit Card Act (Song-Beverly Act), failed to move forward in California's state Assembly after passing the Senate in January by a vote of 21 to 13. S.B. 383, introduced by California State Senator Hannah-Beth Jackson (D-Santa Barbara), would restrict the information that entities may collect in online credit card transactions involving electronic downloadable products, but would permit such information collection to help address fraud and identity theft. Opponents of the bill maintained that the legislation would unnecessarily restrict the collection of information in online commerce.

The bill was introduced in response to a 2013 California Supreme Court decision that held that California's Song-Beverly Act does not apply to online transactions where a product is electronically downloaded.[9] The Song-Beverly Act regulates credit card transactions and, with a few exceptions, limits the requesting or requiring any personal information to be recorded as a condition of accepting a credit card.

Four States Enact New Breach Notification Laws

Several states passed new breach notification laws. Florida and Iowa both amended their existing laws, while Kentucky enacted its first. All three of these laws took effect in July. California also

[9] *Apple Inc. v. Superior Court of Los Angeles County*, 292 P.3d 883, 56 Cal. 4th 128 (Cal. 2013).

passed an amendment to its breach notification, data security, and social security number marketing laws. With the addition of Kentucky there are now 49 breach notification laws in the United States.

Florida. The Florida amendments are extensive, replacing the former statute with a new section in the state code. The new law expands the definition of the term "personal information" to include usernames or email addresses in combination with passwords or security questions, as well as information related to health insurance. The new law also extends the trigger for notification from "unauthorized acquisition" to "unauthorized access." Florida shortened the timing of resident notification from 45 to 30 days, and added a requirement to report breaches (as well as findings of no risk of harm) to the Florida Attorney General for breaches involving more than 500 residents. The law took effect July 1, 2014.

Iowa. Iowa clarified that a "breach of security" includes unauthorized acquisition of personal information in any medium, including paper. Iowa also expanded the scope of personal information to include encrypted records when the method to unencrypt the records was also obtained in the breach. The new law imposed a new requirement to report breaches affecting over 500 residents to the Iowa Attorney General. These amendments took effect July 1, 2014.

Kentucky. The new Kentucky law mirrors many of the other breach notification laws in the country. For example, it limits the definition of the term "personally identifiable information" to an individual's first name or first initial and last name in combination with social security number, driver's license number, or financial account information. The law is triggered by unauthorized acquisition of covered data and requires notification to be made in an expedient manner. The law took effect July 15, 2014. A separate law set out breach notification requirements for Kentucky's governmental agencies.

California. The California law (AB 1710), which passed on August 25, 2014, amends current legal requirements for data breach, data security, and use of social security numbers for marketing purposes. First, entities that "maintain" personal information, not just those that own or license such data, must maintain reasonable data security procedures. Second, the law requires an entity that is the source of a breach that included social security, driver's license, or California identification numbers to include language in the notice offering twelve months of free identity theft protection. Finally, the amended law will bar entities from selling, or offering to sell, social security numbers for marketing purposes. The bill has been sent to the Governor of California, and if signed, would take effect January 1, 2015.

Electronic Privacy Amendment Added to Missouri Constitution

On August 5, 2014, voters in Missouri approved a state constitutional measure that extends protection from unreasonable searches and seizures to "electronic communications and data." The state constitution already provides protection for individuals' "person, papers, homes or effects." The amendment, which passed with near 75% voter approval, requires law enforcement to obtain a warrant in order to gain access to emails, text messages, cloud storage, and other communications or data.

With the passage of the amendment, Missouri became the first state in the nation to extend Fourth Amendment protections to electronic communications and data, the implications of which have yet to be seen. As the new regime takes hold the courts will play a role in interpreting and applying the amendment to law enforcement activity. It is also not known yet whether adoption of the amendment in Missouri will lead to similar attempts in other states.

International

EU "Cookie Sweep" Initiative

The French Data Protection Authority (CNIL) announced that between September 15 and 19, European Union (EU) data protection authorities will conduct a "sweep" of websites to review compliance with the EU Cookie Directive. "Sweeps" are described by the EU as "simultaneous, coordinated checks to identify breaches of consumer law and to subsequently ensure its enforcement."[10]

In this case, the sweep will be an EU-wide screening of websites to assess whether the sites provide consumers with notice and acquire consent to cookie practices in accordance with the EU Directive. Following the sweep, the national data protection authorities could undertake enforcement actions, such as contacting companies about irregularities and seeking corrective or legal action. To date, EU data protection authorities have revealed scant details about the upcoming sweep, particularly whether it is primarily informational or investigative in nature. The sweeps follow a similar effort in May 2013, by the Global Privacy Enforcement Network, in conjunction with 18 data protection authorities, which led to an "Internet privacy" sweep that examined the presence, location, and substance of website privacy policies.

CNIL has announced plans to conduct further examinations of websites in October, 2014, to assess compliance with French data

[10] http://ec.europa.eu/consumers/enforcement/sweeps/index_en.htm.

protection laws, and specifically guidance issued by CNIL in December 2013.

The UK House of Lords Calls the "Right to be Forgotten" Unworkable

On July 25, 2014, the United Kingdom's House of Lords European Union Home Affairs, Health and Education Sub-Committee published a report, titled "EU Data Protection Law: A 'Right to be Forgotten'?" (Report), criticizing the recent European Court of Justice's (ECJ) opinion that found a "right to be forgotten" for European Union (EU) citizens. The ruling would require search engines to delete certain information from their indices. As an initial matter, the Report found that the 1995 Data Protection Directive upon which the ECJ based its opinion to be out of date. The Report also warns against making information that is available to rest of the world unavailable in the EU, as such a practice could have adverse economic and social effects on citizens. Chairman of the Sub-Committee Baroness Prashar summarized the Report by stating, "We do not believe that individuals should be able to have links to accurate and lawfully available information about them removed, simply because they do not like what is said."

The Report described two main reasons the "right to be forgotten" is impracticable. First, the Report cited concerns about the impact on small search engines. The Report expressed concern that such a burdensome requirement would stifle innovative growth in that sector. The Report also noted that as it is currently envisioned, the ECJ's opinion could turn companies into *de facto* censors of information, a role that makes both the companies and the public uncomfortable. The Report found that because the opinion gives no guidance for how to determine whether to honor a request for deletion, companies will have to make this call.

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