



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

Winner of *Chambers USA* "Award of Excellence" for the top advertising practice in 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

## ADDITIONAL

### CONTRIBUTORS

**Emilio W. Cividanes**

ecividanes@Venable.com  
202.344.4414

**Tara Sugiyama Potashnik**

tspotashnik@Venable.com  
202.344.4363

**Julia Kernochan Tama**

jktama@Venable.com  
202.344.4738

**Kelly A. DeMarchis**

kademarchis@Venable.com  
202.344.4722

1.888.VENABLE  
www.Venable.com

## In this Issue:

### Industry Developments

- DAA Launches a Consumer Education Campaign

### Heard on the Hill

- House Energy & Commerce Subcommittee Identifies Legislative Priorities for 2012
- Rep. Markey Releases Draft Mobile Device Privacy Bill
- Senate Subcommittee Holds Hearing on Video Privacy
- Cybersecurity Legislation Introduced in Senate

### Around the Agencies

- Federal Trade Commission Targeting Mobile Privacy Issues
- Federal Trade Commission Issues Closing Letter on Hyundai Blog Campaign
- Federal Communications Commission Modifies its Robocall Rules
- Department of Justice Clarifies Position on Internet Gambling Enforcement

### In the Courts

- U.S. Supreme Court Decision in *United States v. Jones*

### International

- European Union Introduces Comprehensive Data Protection Regulation

## Industry Developments

### DAA Launches a Consumer Education Campaign

LEARN WATCH CONTROL FAQ PARTICIPANTS

Your AdChoices

**WILL THE RIGHT ADS FIND YOU?**

Welcome to Your AdChoices, where you're in control of your Internet experience with interest-based advertising. What's interest-based advertising? To put it really, really simply, it's advertising intended for you, based on what you do online. To put it simply with the help of *jackalopes* and *burritos*, we've made a video you can watch [here](#).

The Advertising Option Icon (which, not to be outdone, also has its own video here) is all about transparency and control. Whenever you see the Icon, you'll know two things: (1) You can find out when information about your online interests is being gathered or used to customize the Web ads you see, and (2) you can choose whether to continue seeing these types of ads.

So you're in control of when the right ads find you. [Learn more.](#)

In January 2012, the Digital Advertising Alliance (“DAA”) launched an education campaign to inform consumers about interest-based advertising and how to take greater control of their online privacy. The DAA is a coalition of the nation’s leading media and marketing trade associations, including the Association of National Advertisers, the American Advertising Federation, the American Association of Advertising Agencies, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative. The DAA administers a self-regulatory program that calls for entities engaged in online behavioral advertising to provide enhanced transparency via the Advertising Option Icon and consumer control.



The campaign, known as “Your AdChoices,” was created pro bono by the Salt Lake City office of MRM, a member of McCann Worldgroup. The campaign builds upon the DAA’s two-and-a-half year effort to develop and implement cross-industry best practices and effective solutions for providing notice and choice with respect to collection and use of data through its Advertising Option Icon (see image to the left).

The campaign includes banner advertising that links to an information website, [www.youradchoices.com](http://www.youradchoices.com), which features three educational videos and a user-friendly consumer choice mechanism. The consumer choice page enables consumers to opt out of interest-based advertising from the companies that participate in the DAA’s Self-Regulatory Program. Companies that participate in the Program are donating ad inventory space to deliver the banner ads to consumers across the Internet. DAA expects to deliver hundreds of millions of ad impressions in 2012.

## Heard on the Hill

### House Energy & Commerce Subcommittee Identifies Legislative Priorities for 2012

Rep. Bono Mack (R-CA), Chairman of the Commerce, Manufacturing, and Trade Subcommittee of the House Energy and Commerce Committee, recently identified her priorities for the Subcommittee for 2012. She said the Subcommittee will continue to examine Internet privacy issues and to evaluate whether legislation is necessary. In 2011, the Subcommittee held several hearings on consumer privacy and data security. Chairman Bono Mack is expected to continue to press to move the SAFE Data Act – a data breach notification bill she introduced last year.

Other priorities for the Subcommittee include stimulating manufacturing in the United States, creating new jobs, and spurring innovation. The Subcommittee will also focus on streamlining the U.S. government’s federal agencies and regulatory codes. The Subcommittee will explore ways to eliminate unnecessary regulation to foster a business friendly environment.

### Rep. Markey Releases Draft Mobile Device Privacy Bill

In the wake of questions about software developed by CarrierIQ, Congressman Ed Markey (D-MA) has prepared a draft “Mobile Device Privacy Act.” As drafted, the legislation would task the Federal Trade Commission (“FTC”) with setting a host of regulations on “monitoring software” for mobile phones.

The bill defines “monitoring software” broadly, as software that “has the capability automatically to monitor the usage of a mobile telephone or the location of the user and to transmit the information collected to another device or system, whether or not such capability is the primary function of the software or the purpose for which the software is marketed.” The bill would apply even if the software is not activated or used. However, information transmitted from a phone to that phone’s commercial mobile or mobile broadband service provider would be excluded.

Within one year, the FTC would be required to promulgate regulations requiring clear and conspicuous disclosures to consumers about “monitoring software” installed on mobile phones. These disclosures would be provided at the time of device sale, service sale, or software installation, and would be provided by phone vendors, service providers, phone manufacturers, operating system providers, or website and online service operators as appropriate.

The FTC would also promulgate regulations requiring such companies (1) to obtain consumers’ prior express consent to any data collection or transmission by such software; (2) to establish an information security program for any data received from such software; and (3) to file, with both the FTC and Federal Communications Commission (“FCC”), a copy of any contract for sharing data from such software between companies.

The bill would create a private right of action allowing plaintiffs to seek up to \$1,000 in statutory damages for each violation, or treble damages for willful or knowing violations. The new requirements could also be enforced by state authorities, the FTC, and the FCC.

### Senate Subcommittee Holds Hearing on Video Privacy

The Senate Judiciary Committee’s Subcommittee on Technology, Privacy and the Law held a hearing on “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century” on January 31, 2012. The hearing follows House passage of H.R. 2471, which would amend the Video Privacy Protection Act (“VPPA”). The VPPA generally prohibits the disclosure of certain customer records by a “video tape service provider.” Under the House legislation, the VPPA would allow consumer consent to the disclosure of video rental records to be obtained online in advance of the disclosure, either for a set period of time or until the consent is withdrawn. The request for consent would be presented separately from other contract forms.

At the hearing, Sen. Leahy (D-VT) and Sen. Franken (D-MN) both expressed interest in updating the VPPA and specifically in extending the law to streaming video. Sen. Franken and Sen. Coburn (R-OK) joined in voicing concern that H.R. 2471 does not address whether companies can make it difficult for users later to revoke consent, and explored alternative consent models in their questions to witnesses. Sen. Franken also said that there may be a need to clarify that the VPPA private right of action can be used to enforce the law’s data retention provisions.

### Cybersecurity Legislation Introduced in Senate

On February 14, 2012, S. 2105, the Cybersecurity Act of 2012, was introduced by Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman (Ind.-CT); Ranking Member Susan Collins (R-ME), Commerce Committee Chairman Jay Rockefeller (D-WV), and Select Intelligence Committee Chairman Dianne Feinstein (D-CA).

The proposed Act does not include the controversial Internet “kill-switch” provision that hampered previous cybersecurity legislation. It keeps with the spirit of earlier legislative proposals by envisioning a public-private partnership for the protection of “critical infrastructure system,” a term broad enough to encompass any “system or asset” designated by the Secretary of the Department of Homeland Security (DHS) pursuant to a procedure set forth in the Act. Critical infrastructure could include any system or asset if damage to it could reasonably result in the interruption of life-sustaining services, catastrophic economic damage to the United States, or severe degradation of national security or its capabilities. Owners/operators who think their systems were wrongly designated would have the right to appeal.

Critical infrastructure would be required to be secured through being regularly

informed of cyber risks and threats, implementing measures that best satisfy cybersecurity performance requirements, and reporting significant cyber incidents affected covered critical infrastructure. The owners of a covered system would determine how best to meet the performance requirements and verify compliance, either by using a third party assessor or through self-certification. DHS would work with the owners and operators of designated critical infrastructure to develop risk-based performance requirements, looking first to current standards or industry practice.

The bill would consolidate power under DHS in a unified office called the National Center for Cybersecurity and Communications. It would also reform the Federal Information Security Management Act (FISMA), which governs the federal government's civilian systems.

## Around the Agencies

### Federal Trade Commission Targeting Mobile Privacy Issues

The Federal Trade Commission ("FTC") has continued to take an active interest in mobile privacy issues, especially with regard to children. Mobile payments and mobile commerce are likely to be another focus of this ongoing effort, with the FTC Bureau of Consumer Protection recently transferring its team for mobile issues into its Division of Financial Practices.

#### Report Critiques Disclosures for Mobile Apps Aimed at Children

On February 16, 2012, the FTC released a staff report on children's mobile applications ("apps"), summarizing its conclusions in the title: "Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing." Intended to be part of a "warning call" to industry on the need to provide better information to parents, the report reviewed hundreds of promotional pages for apps available for children through online markets offered in app stores to determine what information was provided about the apps' data collection and sharing capabilities. The survey also covered apps' social media, rating, and parental control features. The FTC says that it will be conducting additional reviews in the coming months to determine whether some of the apps are violating the Children's Online Privacy Protection Act.

The report states that all members of the mobile ecosystem should play an active role in providing parents with easy access to basic information about data practices, and recommends that:

- App developers should provide simple and short disclosures or icons to provide notice of certain activities; and
- App stores should provide a more consistent way for developers to present this notice to parents.

Recognizing the challenge of providing disclosures within the small screen size of mobile devices, staff stated that this topic will be addressed as part of the FTC's planned workshop on updating its "Dot Com Disclosure" guides for online notices and disclosures.

#### Warning Letters on Background Screening Apps

The FTC has sent warning letters to the providers of six applications that can be used to obtain background information about individuals, allegedly including criminal history information. The letters expressed concern that such information could be used to make decisions about an individual's eligibility for employment, housing, or credit.

Under the Fair Credit Reporting Act ("FCRA"), companies that assemble or

evaluate certain information on consumers for third party use in making such decisions may be deemed "consumer reporting agencies." As such, companies would have to comply with various legal obligations such as taking reasonable steps to ensure maximum accuracy and providing clients with notice of their FCRA duties. Consumer reporting agencies must also afford consumers copies of reports that are used as a basis for adverse action against them and the ability to contest information believed to be incorrect.

While the FTC stated that it has not determined whether the apps are violating the law, it encouraged the companies to review their products and procedures for legal compliance.

### **Planned Workshop on Mobile Payments**

The FTC will convene a public workshop on April 26, 2012, to discuss mobile payment technologies and their consumer impact.

The agency is accepting public comments in advance of the workshop. The announcement of the workshop set out numerous potential discussion questions on topics such as current mobile payments technologies and business models, risks to consumers of these technologies, data practices, and international perspectives.

### **Federal Trade Commission Issues Closing Letter on Hyundai Blog Campaign**

The Federal Trade Commission ("FTC" or "Commission") issued a closing letter on November 16, 2011, to Hyundai Motor America ("Hyundai"), ending its investigation into the company's blogging campaign that was intended to build interest in advertisements scheduled to premiere during the Super Bowl. The investigation had focused on whether bloggers, who were given gift certificates as an incentive to promote the Hyundai videos and comment on the advertisements, were or were not told to disclose to readers that they had received such compensation for their recommendations. The Commission initiated its investigation under the auspices of section 5 of the FTC Act, which the FTC interprets to require disclosure of a material connection between an advertiser and endorser when that relationship would not otherwise be apparent from the endorsement.

Without declaring that no violation of section 5 had occurred, the Commission ultimately closed the investigation after determining the following:

- Hyundai did not know in advance that the gift certificates would be used as incentives, and of the few bloggers who received the gift certificates, some disclosed the incentive.
- An employee of Hyundai's media firm, and not Hyundai, offered the incentives, which were contrary to the social media policies of both Hyundai and the media firm. (Hyundai's social media policy requires bloggers to disclose compensation they receive.)

The Commission also noted that the media firm had been quick to address the conduct of its employee.

The FTC's Hyundai closing letter marks at least the fourth instance in which the FTC has investigated endorsement issues under its revised Guides Concerning the Use of Endorsements and Testimonials in Advertising. In 2010, the FTC investigated Ann Taylor Stores Corp. for providing bloggers with gifts with the expectation that they would blog on a division of the company. The Commission eventually issued a closing letter and chose to forego seeking an enforcement action after finding that: the event where bloggers were provided with gifts was a one-time occurrence; some bloggers disclosed that they had received an incentive to blog (and a posted sign at the event had asked bloggers to disclose the gifts); and the company had adopted a written policy after the event requiring bloggers

to disclose receipt of incentives. Also in 2010, the Commission settled two cases involving allegedly misleading endorsements. In the first case, the FTC settled with Legacy Learning Systems Inc. for engaging online affiliate marketers to pose as consumers who wrote product reviews without disclosing that they were paid for sales from their reviews. In the second case, the Commission settled with Reverb Communications, Inc. after its employees posed as consumers and wrote reviews about the company's products without disclosing their connection to the company.

### Federal Communications Commission Modifies its Robocall Rules

On February 15, 2012, the Federal Communications Commission ("FCC") issued a Report and Order (the "Order") revising the FCC's autodialed and prerecorded telemarketing call regulations to conform with the Federal Trade Commission's ("FTC") analogous Telemarketing Sales Rule ("TSR"). To harmonize the FCC and FTC rules, the FCC has adopted the following requirements, which now set the standard for autodialed and prerecorded telemarketing calls (collectively, "robocalls"):

- Prior express written consent for telemarketing robocalls to wireless numbers and residential lines, even where the caller and consumer have an established business relationship ("EBR");
- Implementation of an automated, interactive opt-out mechanism for telemarketing robocalls, which would allow a consumer to opt out of receiving additional calls immediately during a robocall;
- Adoption of a three percent call abandonment rate for each calling campaign, so that telemarketers cannot shift abandoned calls to certain campaigns, as is possible if calculation is made across multiple calling campaigns; and
- Exemption of prerecorded calls to residential lines made by health care-related entities governed by HIPAA.

The revised rules do not affect existing FCC requirements for prerecorded informational calls, such as calls by or on behalf of tax-exempt non-profit organizations, political calls, and calls for other noncommercial purposes. These calls continue to require some form of prior express consent if placed to wireless numbers.

The revised rules will become effective based on the following schedule once the new rules are published in the Federal Register:

- Twelve-month period for implementation of the "prior written express consent" requirement for autodialed or prerecorded telemarketing calls or messages to wireless or residential lines.
- Twelve-month phase out for the existing EBR exemption for autodialed or prerecorded telemarketing messages to residential wirelines.
- 90-day period for implementation of the automated, interactive opt-out mechanism requirements.
- 30-day period for implementation of the revised abandoned call rule.

### Department of Justice Clarifies Position on Internet Gambling Enforcement

The Office of Legal Counsel for the Department of Justice ("DOJ") has released a memorandum opinion repudiating its long-standing position on the applicability of the Wire Act to certain forms of internet gambling. The DOJ has now taken a position that intrastate online gambling other than sports betting, including poker

and casino games, should no longer face criminal liability under the federal Wire Act.

The question at issue was whether proposals by New York and Illinois to sell lottery tickets online potentially violate the Wire Act. The Wire Act (18 U.S.C. § 1084) prohibits using an interstate wire communications facility, such as the telephone or Internet, to transmit “bets or wagers on any sporting event or contest.” Although one court concluded that the Wire Act only applies to gambling on sporting events or sporting contests, i.e., sports wagering, the DOJ has consistently maintained the public position that the statute applies more broadly to any form of Internet gambling, including online poker and casino games. Due to the nature of the Internet, the New York and Illinois proposals, although intended to be intrastate, may involve out-of-state Internet transmissions, to payment processors located out of state, for example, or simply in the form of incidental transmissions of information that cross state lines.

The new memorandum now takes the position that the statute’s prohibition is “more natural[ly]” read as only applying to sporting events and contests, and that this interpretation is consistent with the legislative history of the Wire Act.

The DOJ memorandum comes at a time when more states are considering intrastate, online gambling as a potential revenue stream. Nevada promulgated regulations at the end of 2011 that pave the way for licensed online intrastate gambling. Other jurisdictions, such as the District of Columbia and New Jersey, have also expressed interest in creating legal online gambling within their own borders.

## In the Courts

### U.S. Supreme Court Decision in *United States v. Jones*

In *United States v. Jones*, a Fourth Amendment case pertaining to government surveillance, the U.S. Supreme Court on January 23, 2012, held that the government’s installation of a GPS tracking device on a vehicle without the appropriate warrant, and the government’s use of that device to monitor that vehicle’s movement, constituted a search. Justice Scalia, writing for the majority and joined by Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor, found that the government had conducted a search in violation of the Fourth Amendment when the police physically intruded on the defendant’s private property by installing a GPS device on the defendant’s car as part of the government’s efforts to gather evidence of drug possession and distribution. Although the government had earlier applied for a warrant, the GPS device was not installed until after the expiration of the warrant. Based on evidence obtained through the surveillance, the defendant was convicted. Rather than rely on the most recent Fourth Amendment jurisprudence, which has centered on whether the government violated a person’s “reasonable expectation of privacy,” the majority focused on the Court’s earlier emphasis on physical trespass. By doing so, the majority found that the physical intrusion to the car with the installation of the GPS device and the obtaining of information were sufficient to constitute an unconstitutional search.

In the concurring opinion, written by Justice Alito and joined by Justices Ginsburg, Breyer, and Kagan, the minority agreed that a Fourth Amendment violation had occurred, but took the position that that the case should have been analyzed through the “reasonable expectation of privacy” lens. The minority found that short-term surveillance on public streets would be reasonable, but that longer-term use of GPS monitoring would not comport with society’s reasonable expectation of privacy. The minority noted that privacy expectations can evolve as technology changes, and observed that some people may value the tradeoff of increased convenience at the expense of privacy. The minority concluded, however, that “[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”

In an additional concurrence, Justice Sotomayor, who joined the majority, also wrote that in this digital age, it may be time to revisit the notion that a person has no reasonable expectation of privacy in information that he or she discloses to a third party. She expressed doubt that the public would accept disclosures of lists of websites people had visited to the government without a warrant.

## International

### European Union Introduces Comprehensive Data Protection Regulation

On January 25, 2012, the European Commission (the “EC”) formally unveiled its proposed “General Data Protection Regulation” (the “Regulation”). In its current form, the Regulation proposes sweeping changes to many of the fundamental tenets of the European Union’s (“EU”) 1995 Data Protection Directive.<sup>1</sup>

Like the 1995 Directive, the Regulation is intended to provide a comprehensive approach for the entire EU. It would replace the 1995 Directive. The proposal’s status as a “Regulation” means it would become directly binding on all EU Member States upon passage. The stated purpose for using this vehicle is to “reduce legal fragmentation and provide greater legal certainty” and to harmonize the rules across Member States.

The Regulation has two parts—(1) a General Data Protection Regulation that would govern the protection of individuals with regard to the processing of personal data and the free movement of such data, and (2) a proposal directed towards “competent authorities” regarding the processing of personal data in connection with the investigation and prosecution of crimes.

The Regulation would maintain the long standing rights under the 1995 Directive for notice of data collection, as well as data access and correction rights. The Regulation also contains significant changes. Among these changes, the Regulation would implement the long-discussed “right to be forgotten.” This would give the data subject the right to have personal data erased if the data is no longer necessary for the purposes for which it was collected or processed, if consent is withdrawn, if the storage period consented to has expired where there is no other legal ground for the data processing, if the data subject objects to processing, or if the processing does not comply with the Regulation. The Regulation also introduces a right of “data portability.” Data subjects would be legally entitled to obtain an electronic copy of their personal data in a commonly used format that allows for further use.

The definition of “the data subject’s consent” is modified in the Regulation to require “freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement....”. (Art. 4.)

The Regulation would expand many of the obligations now imposed upon data controllers to data processors as well. These obligations would also be imposed on data controllers located outside of the EU, if their processing activities are related to “the offering of goods or services” to EU data subjects, or “the monitoring of their behaviour.” (Art. 3.)

In addition, the Regulation would impose a data breach notification requirement in the EU, requiring data controllers “without undue delay and, where feasible” to notify the local Data Protection Authority (DPA) of a data breach. Notification made outside a 24-hour window would require a “reasoned justification” for the delay. Notification would not be required if the controller demonstrates to the DPA that the data is subject to appropriate technological protection measures, i.e., if it was encrypted in some fashion. Notification to individuals would be

---

<sup>1</sup> The Regulation and documents in support are available here: [http://ec.europa.eu/justice/newsroom/data-protection/news/120125\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm).

required where the breach is likely to adversely affect the protection of personal data or privacy of the data subject. (Art. 32.)

Now that the Regulation has been formally proposed by the EC, there are still several steps in the process for adoption. The European Parliament and the Council (comprised of the governments of EU Member States) will review it and propose amendments. This cycle will repeat once more until the parties agree on amendments or convene a "conciliation committee" to try to find a solution. Either the Parliament or the Council can block the proposal if there is still no agreement on the joint text proposed by the conciliation committee. If not blocked, the proposal would go into effect two years after adoption.

\*\*\*\*\*

### 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.

© 2012 ATTORNEY ADVERTISING The Download is published by the law firm of Venable LLP. Venable publications are not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations. You are receiving this communication because you are valued client or friend of Venable LLP. Questions and comments concerning information in this newsletter should be directed to Stuart Ingis at [singis@Venable.com](mailto:singis@Venable.com).