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

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

Ariel S. Wolf
awolfVenable.com
202.344.4464

www.Venable.com

October 2013

In this Issue:

Heard on the Hill

House Bipartisan Working Group Considers Privacy

On September 26, 2013, the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") held the first of a series of meetings of the new bipartisan Privacy Working Group ("Working Group"). The Working Group was convened by Chairman Terry Lee (R-NE) to examine consumer privacy in order to identify issues to be recommended for formal consideration by the Subcommittee. The Working Group is co-chaired by Reps. Marsha Blackburn (R-TN) and Peter Welch (D-VT) and includes the following Subcommittee members: Rep. Joe Barton (R-TX), Rep. Pete Olson (R-TX), Rep. Mike Pompeo (R-KS), Ranking Member Jan Schakowsky (D-IL), Rep. Bobby Rush (D-IL), and

Rep. Jerry McNerney (D-CA). Rep. Blackburn has indicated that the Working Group will meet once a week while Congress is in session until the end of the year.

The first meeting was an education briefing involving industry representatives from Google, Wal-Mart, and BlueKai. The Working Group discussed how data empowers marketing and advertising and inquired into how companies address consumer privacy interests. The discussion focused on the type of data collected and used for marketing purposes, the channels through which data is collected, and how data benefits consumers.

The second meeting of the Working Group was scheduled to be held early in October but has been postponed because of the federal government shutdown.

Around the Agencies

New TCPA Rules Effective October 16, 2013

The Federal Communications Commission's ("FCC") previously issued rules on the consent requirement under the Telephone Consumer Protection Act ("TCPA") went into effect on October 16, 2013. The prior rule prohibited using prerecorded voice calls, or an autodialer to call or text a wireless phone for telemarketing purposes unless the caller had obtained the "prior express consent" of the called party. There was no exception for an "established business relationship" between the parties[1]. After October 16, the FCC now requires a higher standard of consent—prior express written consent[2]. The FCC has stated that the new rules are intended to achieve maximum consistency with the Federal Trade Commission's ("FTC") analogous Telemarketing Sales Rule ("TSR").

In order to be considered sufficient, the prior express written consent must:

1. be in writing;

2. bear the signature of the person called;

3. list the phone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered; and

4. contain a clear and conspicuous disclosure informing the

1 47 C.F.R. § 64.1200(a)(1).
2 *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 2 (2012) *(2012 TCPA Order).*

signatory that:

(a) by executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial voice; and

(b) the person is not required to sign the agreement (directly or indirectly), or to enter into such an agreement as a condition of purchasing any property, goods, or services.

The notice must also be separate and distinguishable from advertising copy or other disclosures. Written consent may be obtained through methods that comply with the E-SIGN Act, such as email, websites, text message, telephone keypress, or voice recording. Previous non-written consent obtained previously to October 16 does not carry over.

FTC to Hold Workshop on Native Advertising

In September the Federal Trade Commission ("Commission" or "FTC") announced that it would convene a December 4, 2013 workshop in Washington, DC on "native advertising." "Native advertising," or "sponsored content," is the phrase used by the Commission to refer to the practice of blending ads with news, entertainment, and other content in digital media. The workshop is intended to bring together representatives of industry, consumer advocates, academics, and regulators to examine how native advertising is presented to consumers and whether they recognize such paid messages.

Potential workshop panel topics were expected to cover:

- The origin of the wall between regular content and advertising (and the challenges of maintaining this in digital media).
- How paid messages are integrated into regular content (and how this differs with mobile devices).
- The entities that control the presentation of sponsored content.
- How ads are differentiated from content.
- What the research says about how consumers understand paid advertising that is integrated into content.

Formal requests to participate in the workshop were originally due October 29. Upon the shutdown of the federal government, the FTC announced that all public workshops were postponed until further notice. It remains to be seen whether the October deadline will be extended and whether this specific workshop will take place as originally planned.

New HIPAA Regulations Now in Effect

As of September 23, 2013, the Department of Health and Human Services ("HHS") expects full compliance with its significant revisions to its privacy, security, and data breach regulations originally issued under the Health Insurance Portability and Accountability Act ("HIPAA") and revised under the Health Information Technology for Economic and Clinical Health Act ("HITECH"). All affected entities should have completed their transition to the new requirements, including those related to privacy notices, contracts, policies and procedures, training, and breach notification.

HHS continued to issue important new guidance in the days before the compliance deadline. Notably, HHS released model privacy notices for health plans and health care providers that reflect the requirements of the new regulations. The models are available in booklet, full page, "layered," and text versions and are accompanied by instructions. In addition, HHS announced a 45-day enforcement delay until November 7, 2013, for provisions of the HIPAA rule applying to refill reminders and other paid communications about individuals' prescriptions. HHS also issued new guidance on these provisions on September 19, 2013. Other new guidance issued in September addressed decedents' privacy and student immunizations.

In the States

California Privacy Ballot Initiative

This past summer and early fall have been an active time for privacy developments in California, including, among other items, the filing and subsequent withdrawal of a ballot initiative. The privacy ballot initiative, named the Personal Privacy Protection Act by its sponsors, former state Senator Steve Peace and attorney Michael Thorsnes, sought to change the treatment of personally identifying information ("PII") by amending the California state constitution. Specifically, the ballot initiative would have created new restrictions and obligations on the supplying, collecting, and disclosure of PII when it is collected for commercial or governmental purposes. With limited exceptions, the ballot initiative would have created a presumption that PII is confidential and that any disclosure of the information creates harm to the person who supplied the

information unless that person authorized the disclosure (i.e., opts-in).

In September, the state's fiscal assessment of the ballot initiative found that although the fiscal impact on California was unknown, it could potentially impose significant costs in the form of costly lawsuits, an increased court workload, data security improvements, and changes to data practices. Supporters of the ballot initiative had received approval to collect the 807,615 signatures needed from registered voters by February 2014 to have the ballot initiative placed on the November 2014 ballot; however, following the release of the fiscal assessment, the ballot initiative supporters withdrew the initiative.

California's AB 370 – Do Not Track Disclosure Law

On September 27, 2013, California Governor Jerry Brown signed A.B. 370 into law, which changes the state's online privacy policy disclosure requirements. Under current law and state attorney general interpretation, operators of websites, online services, and mobile apps must post privacy policies that include: (1) categories of PII collected through their service, (2) categories of third parties with whom the operator may share PII, (3) how a consumer may review and request changes to PII collected through the service (if such a process is maintained), (4) how operators notify consumers of material changes to the privacy policy, and (5) the effective date of the privacy policy.

Under the new law, operators (e.g., web publishers) will now be required to disclose whether other parties (i.e., ad networks, analytics providers) may collect PII about a consumer's online activities over time and across different sites when the consumer uses the operator's service. Those other parties will also be required to describe and disclose in their own privacy policies how they respond to browser "do not track" ("DNT") signals or other mechanisms that provide consumers with a choice regarding PII collection. The law becomes effective January 1, 2014.

California Breach Notification Law Extended to Online Log-in Credentials

On September 27, 2013, California's governor signed S.B. 46, a bill that expands the reach of the state's existing data breach law to cover consumers' online log-in credentials. Businesses and state agencies that own or license computerized data with personal information already must disclose security breaches to any resident of California whose personal information had been compromised. Existing law defined "personal information" to include a person's name in combination with that person's

social security number, driver's license number, California identification card, account number or credit or debit card number in combination with any security code or password, medical information, or health insurance information. The new law creates a separate category of personal information that includes a consumer's "user name or email address, in combination with a password or security question and answer that would permit access to an online account."

For breaches involving only this new category of personal information, the law allows businesses to notify consumers in electronic form or any other form that directs consumers to change their passwords and security questions or otherwise protect their online accounts. At the same time, the new law prohibits companies from providing notification of log-in breaches to a consumer's compromised email address, unless the person is connected from the location that the company knows the person customarily accesses the account from. If not by email, notification must take place through alternative means allowed under existing California law, such as through writing, conspicuous posting on the business's website, or notification to major statewide media. A business may also comply through the exercise of its own information security policy that is otherwise consistent with the law's timing requirements.

International

Vote Scheduled on EU General Data Protection Regulation for October 21, 2013

News on the European Union Draft General Data Protection Regulation ("Regulation") continues to trickle out of the EU, reflecting the minimal progress made on passing the draft Regulation to date. At present, the draft Regulation, which would replace the current European data protection framework in its entirety, remains stalled on major substantive principles. Nevertheless, a vote by the lead committee, the LIBE (Civil Liberties Committee), has been scheduled for October 21, 2013 after previously being postponed on two occasions as the LIBE struggled to reduce the over 3000 amendments that have been proposed for the draft. This vote would determine the LIBE's position and is a prerequisite for negotiations between the European Parliament and Council to commence.

The most recent news reflects the result of meetings on October 7 between the Ministries for Justice and Home Affairs of the 28 EU Member States, which gathered in Luxembourg to discuss the "one-stop-shop" principle that is a foundational principle of the draft. Under current law, multinational companies established in several EU countries are required to comply with

the local requirements in each country where they are established. The "one-stop-shop" would hold that the local data protection authority in the country's primary "establishment" would be responsible for all of the company's activities. The one-stop-shop would also make the EU act as a single entity for enforcement purposes. Different member states, however, feel that the one-stop-shop would create forum shopping among multinational companies. After the October 7 meeting, the Council issued a press release noting that "expert work should continue" to flesh out a model that would satisfy more member countries while preserving the concept.

The publicly stated goal remains to present a compromise text in December 2013, with a vote taken before the European elections are held in May 2014. It remains to be seen whether that aggressive timetable will be met.

****

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.

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

VENABLE® LLP