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

1.888.VENABLE
www.Venable.com

DECEMBER 2011

In this Issue:

Regulators and policymakers are expected to continue their examinations of privacy and data security issues in 2012. It is anticipated that both the Department of Commerce and the Federal Trade Commission ("FTC") will issue privacy reports early in the new year as follow ups to their respective preliminary reports issued in December 2010. The Department of Commerce will likely renew its call for a consumer bill of rights and for industry to development of voluntary codes of conduct. The FTC's report will likely promote enhanced privacy including greater transparency, uniform choice, and "privacy by design." Both reports will inform and influence the debate on privacy.

In this issue of the Download, we report on recent developments including the release of Digital Advertising Alliance's new self-regulatory principles for Multi-Site Data; congressional examinations of privacy, online gambling, and cybersecurity; the FTC's review of the Children's Online Privacy Protection Act; and a recent FTC settlement involving Facebook.

Marketplace Developments

DAA Announces Comprehensive Principles for Online Collection of Web Data

In November 2011, the Digital Advertising Alliance ("DAA") released the Principles for Multi-Site Data ("Principles"). These new principles expand the scope of self regulation of online data collection. The DAA has previously developed cross-industry best practices for consumer choice in online behavioral advertising (OBA) through its Advertising Option Icon program.

The DAA includes the American Association of Advertising Agencies (4A's), the American Advertising Federation (AAF), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB), and the Network Advertising Initiative (NAI), and includes more than 400 participating companies. To learn more about the DAA, visit www.aboutads.info.

The new Self-Regulatory Principles establish comprehensive self-regulatory standards governing the collection and use of Multi-Site Data, which the DAA has defined as data collected from a particular computer or device regarding Web viewing over time and across non-affiliated Web sites. The Principles establish a framework governing the collection of online Multi-Site Data that also defines when companies must provide transparency and choice, beyond the existing requirements for OBA. The Principles also codify existing industry best practices restricting the collection or use of Multi-Site Data for the purpose of any adverse determination concerning employment, credit, health treatment or insurance eligibility. Like the original OBA Principles, the new principles apply across the entire Internet ecosystem and will deliver greater transparency and control to consumers. The Multi-Site Principles are intended to be implemented in 2012.

The new Principles consist of the following specific requirements:

- **Transparency and consumer control for purposes other than OBA –** The Principles call for organizations that collect Multi-Site Data for purposes other than OBA to provide transparency and control, except for certain operations and systems management purposes, market research and product development, or where such Multi-Site Data is reasonably de-identified.

- **Collection / use of data for eligibility determination –** The Principles call for organizations not to collect, use or transfer Multi-Site Data for the purposes of determining a consumer's eligibility for employment, credit standing, healthcare treatment and / or insurance underwriting or pricing.

- **Collection / use of health and financial data –** The Principles call for organizations not to collect Multi-Site Data that contains certain health or financial data about a specific

individual without that individual's opt-in consent.

- **Collection / use of children's data –** The Principles recognize that data collected from children merits heightened protection, and therefore provides that Multi-Site Data defined as personal information by the Children's Online Privacy Protection Act (COPPA) should not be collected from children the organization has actual knowledge are under the age of 13 or from Web sites directed to children under the age of 13, except as compliant with COPPA.

- **Meaningful accountability –** The Principles acknowledge that the limitations and restrictions on the collection and use of Multi-Site Data are within the scope of the DAA's Accountability Programs.

Heard on the Hill

House Energy and Commerce Committee Continues to Debate Privacy and Internet Issues

The House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade ("CMT Subcommittee") is nearing the conclusion of the first session of the 112th Congress. Over the course of the last year, the CMT Subcommittee has repeatedly examined issues of privacy and data security, and is expected to continue this trend into the new next year.

Rep. Mary Bono Mack (R-CA), Chair of the CMT Subcommittee, continues to press her data security and breach notification legislation (H.R. 2577). The legislation has been in negotiations for months, and full Committee markup has been repeatedly delayed due to a lack of consensus among Republican members. Competing bills have been put forward by Reps. Stearns (R-FL) (H.R. 1841) and Scott (D-VA) (H.R. 1707), but are unlikely to advance over the Chair's legislation. Meanwhile, the CMT Subcommittee has held several hearings already this Congress on aspects of consumer privacy and is expected to hold additional hearings in the second session.

The CMT Subcommittee has also turned its attention to online gambling issues in two recent hearings. On October 25, 2011, the CMT Subcommittee held a hearing on "Internet Gaming: Is There a Safe Bet?" to examine whether current restrictions on online gambling should be eased. A second hearing on November 18, 2011, entitled "Internet Gaming: Regulating in an Online World," featured testimony from Reps. John Campbell (R-CA) and Barney Frank (D-MA), who have introduced legislation to re-legalize and regulate online gambling. The CMT Subcommittee also heard testimony from Rep. Frank Wolf (R-VA), who opposes easing the ban on online gambling.

House Intelligence Committee Passes Cybersecurity Legislation

The U.S. House of Representatives' Intelligence Committee passed H.R. 3523, the Cyber Intelligence Sharing and Protection Act on December 1, 2011, in an effort to protect the intellectual property of U.S. businesses from cyber attacks. The bill was introduced by committee Chairman Mike Rogers (R-MI) and Ranking Member Dutch Ruppersberger (D-MD) and passed by a 17-1 vote.

The bill would direct the Director of National Intelligence to establish procedures to allow the intelligence community to share cyber threat intelligence with certified entities within the private sector and for granting security clearances to organizations that wish to receive this information. Private sector cybersecurity providers would be limited to using the information they receive to protect themselves or their customers. Entities that "self-protect" from cybersecurity threats may use threat information to protect their own rights and property while also having the right to share it with other entities, including the federal government. The bill would exempt from liability the sharing of cyber threat information in good faith pursuant to the procedures established by authority of the bill or the failure to act on cyber threat information. The bill also would allow private sector entities to share cyber threat information anonymously through an undefined process or restrict with whom they share threat information.

Two amendments to the bill were also passed—the first to improve the privacy protections for cyber threat information by prohibiting the government from using the information for regulatory purposes. The government would also be prohibited even from searching the information, unless for a cybersecurity or national security purpose. The second amendment would require an annual report to Congress outlining the information that the private sector shares voluntarily with the government.

Congressional Privacy Caucus Considers Children's and Teens' Online Privacy

On December 14, 2011, the House Congressional Privacy Caucus ("Caucus") convened its first briefing of the 112th Congress and examined protecting children and teens online. The bi-partisan Caucus is comprised of 25 members from both sides of the aisle and is co-chaired by Rep. Markey (D-MA) and Rep. Barton (R-TX). The Co-Chairs used the forum to promote passage of H.R. 1895, the Do Not Track Kids Act, which Rep. Markey explained would create an opt-in requirement for collection of personal information from anyone under 13 without parental consent and from teens without their consent, create an eraser button, prohibit online behavioral advertising directed at children, and require simple and clear privacy policies.

The panel was comprised of Federal Trade Commission ("FTC") Chairman Jon Leibowitz and FTC Commissioner Julie Brill, as well as representatives from consumer groups and academia. Much of the discussion focused on the Do Not Track Kids Act and the FTC's current review of the Children's Online Privacy Protection Rule

("COPPA Rule"). While the Do Not Track Kids Act would also focus on teens aged 13-17, the scope of the FTC's COPPA Rule review is limited to children under age 13. Several of the panelists expressed support for the Co-Chairs' bill, but the FTC representatives declined to take a position on the bill.

Rep. Markey concluded the forum by noting that the Children's Online Privacy Protection Act of 1998 was passed "BF" ("before Facebook"), and that legislation and regulations were required to update the law.

House of Representatives Passes Update to Video Privacy Protection Act

On December 6, 2011, the House of Representatives approved legislation (H.R. 2471) authored by Rep. Goodlatte that would amend the consumer consent provisions of the Video Privacy Protection Act ("VPPA"). The VPPA, codified at 18 U.S.C. § 2710, restricts the disclosure of information that identifies a person's request or receipt of specific video materials or services from a "video tape service provider," including both sales and rental providers of videos and "similar audio visual materials." A video tape service provider may only disclose such information in certain circumstances, including with the "informed, written consent" of the consumer.

H.R. 2471 would amend the VPPA to specify that such consumer consent can be obtained (1) via the Internet and (2) in advance of the release, either for a set period of time or until the consent is withdrawn. Such advance consent would be an alternative to, not a replacement for, the current VPPA rule that consent must be obtained at the time of the disclosure.

The VPPA also permits the disclosure of consumers' names, addresses, and the subject matter of the video materials for marketing purposes if the video tape service provider has given consumers the opportunity to opt out of the disclosure. H.R. 2471 would not affect this exception.

As amended by the House Judiciary Committee, H.R. 2471 would also require the consent request to be presented to the consumer separately from any other terms. Over 100 members of the House, mostly Democrats, opposed the legislation. The bill now moves to the Senate for consideration.

Around the Agencies

Federal Trade Commission Extends Request for Comments on Proposed Rule to Amend COPPA

In September 2011, the Federal Trade Commission ("FTC" or "Commission") released a proposed rule ("Proposed Rule") to amend the FTC's current Children's Online Privacy Protection Rule ("COPPA Rule"). The COPPA Rule, which implements the Children's Online Privacy Protection Act of 1998 ("COPPA"), applies to operators of commercial websites and online services directed to children under age 13 that collect, use, or disclose personal information from children, and to operators of general audience websites that have

actual knowledge that they are collecting, using, or disclosing personal information from children under age 13. The COPPA Rule provides parents with tools to control how information about their children is collected online. Comments were originally due November 28, 2011. The Commission has since extended the deadline for comments until December 23, 2011.

When the Commission released the Proposed Rule, it explained that it was seeking to update the regulation to help ensure that it continues to protect children's privacy online as technologies evolve. The FTC typically conducts a review of its regulations once every decade. In the case of the COPPA Rule, the Commission conducted a voluntary review in 2001 and a statutorily mandated review in 2005, after which time the Commission determined that no changes to the regulation were warranted. In 2010, the FTC decided to conduct a review once again of the COPPA Rule in light of technological advancements, particularly in the mobile arena, and asked for general comments on the regulation without formally proposing a new COPPA Rule. After considering the feedback it received in 2010, the Commission released this latest Proposed Rule to amend the COPPA Rule.

In its proposal, the FTC has explained that the COPPA Rule would continue to apply to children under age 13. Additionally, the Commission has noted that the regulation would still only apply to general audience websites and online services when operators have actual knowledge that they are collecting personal information from children.

Interested parties now have an opportunity to comment on the Commission's many proposed amendments to the COPPA Rule, including among others the Commission's proposals to:

- Expand the definition of "collection"
- Expand the definition of "personal information"
- Consider the presence of child celebrities and celebrities who appeal to children as factors when determining if a website or online service is directed to children
- Modify required online privacy policies and direct parental notices
- Eliminate the sliding scale approach to obtaining verifiable parental consent
- Create a Commission approval process for identifying new means of obtaining verifiable parental consent
- Place data security obligations on service providers
- Implement new data retention and deletion requirements
- Include audit and reporting requirements for self-regulatory safe harbor programs

Federal Trade Commission Announces Settlement with Facebook

On November 29, 2011, the Federal Trade Commission ("FTC" or "Commission") announced that it had reached a settlement with Facebook over concerns about changes to Facebook's privacy settings that publicly exposed users' personal information as well as other privacy practices related to information sharing by Facebook apps and between Facebook and advertisers.

Under the terms of the settlement, Facebook will be subject to independent audits of its privacy practices for the next 20 years and will be required to obtain affirmative, express consent from consumers before sharing previously collected personal information with third parties in any way that materially exceeds the restrictions imposed by a user's privacy settings. Facebook did not have to provide any monetary compensation.

The FTC's complaint alleges eight separate violations of the FTC Act, which prohibits deceptive and unfair acts or practices. The alleged violations include claims that Facebook's privacy settings did not adequately allow users to control the distribution of their personal information to third parties, that changes to Facebook's privacy policy and practices in December 2009 prevented consumers' ability to restrict the sharing of personal information, and that Facebook shared parts of users' profile information with advertisers. The Complaint also made allegations related to information sharing by Facebook apps, and violations of the U.S.-EU Safe Harbor Framework.

The draft consent order does not contain an admission of wrongdoing. The consent order governs "covered information" broadly defined to cover a number of different types of personal data. Facebook is ordered not to misrepresent, in any manner, the extent to which it maintains the privacy or security of covered information, the extent to which users can control the privacy of covered information or make it accessible to third parties, and the extent to which Facebook adheres to the U.S.-EU Safe Harbor.

In addition, Facebook is required to clearly and prominently display notice to users prior to sharing users' nonpublic information with third parties in any manner that exceeds a user's privacy settings. This notice must be separate from Facebook's privacy policy, and must disclose the categories of nonpublic user information that will be disclosed to third parties, the identity or specific categories of these third parties, and that sharing exceeds the user's privacy settings. Facebook will then have to obtain the user's affirmative express consent. If sharing does not materially exceed the restrictions imposed by a user's privacy settings, consent is not necessary.

Facebook has 60 days to implement procedures designed to ensure that covered information from deleted profiles can no longer be accessed by any third party. These procedures must ensure that information from deleted or terminated accounts cannot be accessed by any third party within 30 days of the account termination.

Facebook is also ordered to establish and maintain a comprehensive

privacy program intended to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of covered information. Facebook will be subject to biannual independent assessments for the next 20 years, with the first required within 180 days of the order.

The consent order also includes reporting and compliance provisions, requiring Facebook to file a report within 90 days setting forth the manner of its compliance with the consent order, and is required to provide to the FTC and/or retain different categories of documents, such as all widely disseminated statements that describe information sharing practices and consumer complaints, for designated periods of time.

****

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 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

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

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