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
awolf@Venable.com
202.344.4464

August 2013

In this Issue:

In the Marketplace

Digital Advertising Alliance Releases Mobile Guidance

The Digital Advertising Alliance ("DAA") released guidance on July 24, 2013 that explains how its Self-Regulatory Principles apply in the mobile app and mobile Web environments. The DAA is a consortium of trade associations and companies led by the American Association of Advertising Agencies, the Association of National Advertisers, the American Advertising Federation, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative.

The new mobile guidance is available for download at http://www.aboutads.info/DAA_Mobile_Guidance.pdf

The new mobile guidance makes clear that the DAA's existing Self-Regulatory Principles (i.e., Self-Regulatory Principles for Online Behavioral Advertising and Multi-Site Data) apply consistently across channels to certain data collection practices that may occur on mobile or other devices, and that standards and definitions restated in the mobile guidance should be interpreted consistently across all of DAA's Principle documents. Commentary within the existing Principles also applies in the mobile web site and

application environments where relevant.

The guidance addresses the application of the existing DAA Self-Regulatory Principles in the mobile web site environment and also explains covered entities' obligations with respect to: "Cross-App Data," a term that means "data collected from a particular device regarding application use over time and across non-Affiliate applications;" "Precise Location Data" (as defined in the guidance); and "Personal Directory Data," a term that encompasses "calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a particular device." The guidance extends to the mobile web site and application environments those elements of the existing Self-Regulatory Principles that address sensitive health and financial data, data security, and prohibitions on the use of data for eligibility purposes.

The guidance is now in an implementation period during which the DAA will be educating companies about the guidance and developing (or otherwise specifying) a mechanism or setting that companies can use to implement the Consumer Control Principle with respect to Cross-App Data. During this time, the guidance is not yet in effect or enforceable against companies. This is similar to the implementation period after the initial Self-Regulatory Principles for Online Behavioral Advertising were published, which permitted the DAA to launch its Advertising Options Icon and uniform consumer choice page located at www.AboutAds.info.

Heard on the Hill

House Energy and Commerce Task Force on Privacy

On August 1, 2013, Chairman Lee Terry (R-NE) and Ranking Member Jan Schakowsky (D-IL) of the House Energy and Commerce Committee's ("Committee") Subcommittee on Commerce, Manufacturing, and Trade ("Subcommittee") announced the formation of a new bipartisan Privacy Working Group ("Working Group"). The Working Group has been tasked with examining online privacy matters and the need to protect personal information in a way that preserves and promotes innovation. Specifically, Chairman Terry has asked the Working Group to explore "what we need to fix or if we need to fix anything."1

Representative Marsha Blackburn (R-TN), who also serves as Vice Chair of the Committee, along with Representative Peter Welch (D-VT), have been appointed to co-chair the Working Group. Other

1 Press Release, Terry, Schakowsky Announce Bipartisan Privacy Working Group (Aug. 1, 2013), *available at* http://energycommerce.house.gov/press-release/terry-schakowsky-announce-bipartisan-privacy-working-group.

members of the Working Group include Representatives Barton (R-TX), McNerney (D-CA), Olson (R-TX), Pompeo (R-KS), Rush (D-IL), and Schakowsky (D-IL). These Representatives serve on the Subcommittee, which maintains jurisdiction over privacy matters.

The Working Group is expected to identify areas of common ground and to provide recommendations to the Subcommittee for its consideration. No formal timetable has been announced for the Working Group to complete its work.

House Energy and Commerce Subcommittee Hears from Industry on Reforming Breach Notification Laws

On Thursday, July 18, 2013, Representative Lee Terry (R-NE), Chairman of the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, convened a hearing titled "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers," to examine whether there is a need for federal breach notification legislation.

While stressing the need to reform the patchwork of state data breach laws and to ensure that consumers' data is protected, Chairman Terry cautioned against taking legislative or regulatory action that would add unnecessary compliance costs to the system. Ranking Member Jan Schakowsky (D-IL) called for a national standard for data breach notification and enforcement that would serve as the floor – not the ceiling – for state legislation and enforcement. Representative Joe Barton (R-TX) and Representative Henry Waxman (D-CA), Ranking Member of the full Committee, agreed with Rep. Schakowsky's approach.

Industry witnesses focused on the high cost of compliance with the many breach notification laws and regulations across the country. The industry representatives generally supported a single, technology-neutral federal breach notification standard to replace the patchwork of state laws. Issues such as safe harbor provisions, the scope of personally identifiable information, and notification thresholds were raised but not discussed in detail. The two legal scholars testifying at the hearing discussed several concepts for policymakers to consider for breach notification reform, such as preemption, burdens of proof, and centralization of enforcement.

While other data issues, such as data aggregation and identity theft, were mentioned in passing, the substance of the hearing remained focused on breach notification issues.

The Senate Committee on Commerce Considers Cybersecurity

On July 24, 2013, Chairman Rockefeller (D-WV) and Ranking Member Thune (R-SD) of the Senate Commerce Committee introduced S. 1353, the Cybersecurity Act of 2013. The bill is intended to provide for an ongoing partnership between the public and private sectors to improve cybersecurity, as well as to

increase cybersecurity research, workforce development, and education. Specifically, the bill would amend the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, industry-led set of standards and procedures to reduce cyber risks to critical infrastructure.

The bill does not include information sharing provisions, which have previously drawn the attention of privacy and civil liberties advocates. Instead the bill avoids the information sharing question altogether by prescribing the development of a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to "identify, assess, and manage cyber risks," without providing requirements for what that approach must contain.

The bill currently has the support of different voices in the business community, but its potential for passage remains unclear.

Around the Agencies

Federal Trade Commission Continues to Add to COPPA FAQ Guidance

At the end of July 2013, the Federal Trade Commission ("FTC") released additional guidance on how to comply with the Children's Online Privacy Protection Rule ("COPPA Rule"). Updates to the COPPA Rule were released by the FTC in December 2012, and became effective July 1, 2013. To assist entities with navigating the changes to the COPPA Rule, the FTC began releasing FAQs in its Complying with COPPA: Frequently Asked Questions (A Guide for Business and Parents and Small Entity Compliance Guide) publication in April 2013. Since that time, the FTC has steadily distributed more guidance each month, with the most recent wave of FAQs released in July.

The July updates to the FAQs address the following topics:

- **Actual Knowledge.** FAQs D.10, 11, and 12 provides examples of when a site or service may have "actual knowledge" of collecting personal information on child-directed sites.

- **Share Buttons.** FAQ D.9 provides that verifiable parental consent must be obtained if an app includes embedded buttons or plug-ins that allow children to send email or post information.

- **Information Collected from a Child-Directed Site.** FAQ K.2 is directed to ad networks and provides guidance on how to comply with the COPPA Rule if the ad network discovers that it has been collecting personal information through a

child-directed site.

The FTC has stated that it intends to continue releasing additional FAQs as it receives new inquiries from interested entities.

September Compliance Deadline for New HIPAA Regulations

The compliance deadline for the Department of Health and Human Services' ("HHS") significant revisions to its privacy, security, and data breach regulations is September 23, 2013. The regulations were originally issued under the Health Insurance Portability and Accountability Act ("HIPAA") and the revisions implement changes made under the Health Information Technology for Economic and Clinical Health Act ("HITECH").

By the September deadline, affected entities will be expected to complete their transition to the new requirements including those related to privacy notices, contracts, policies and procedures, training, and breach notification. Among the key changes in the new regulations, business associates – as well as their downstream subcontractors – will now be directly liable under HIPAA for complying with the rules. A new breach notification regime for "unsecured protected health information" also applies. In addition to the substantive changes effected by the new regulations, HHS has the ability to seek higher penalties for HIPAA violations even in instances when an entity is not aware of the violation.

****

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