VENABLE® LLP

the download

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

SEPTEMBER 2008

EDITORS

Emilio W. Cividanes
ecividanes@venable.com
202.344.4414

Stuart P. Ingis
singis@venable.com
202.344.4613

CONTRIBUTORS

Ellen Traupman Berge
etberge@venable.com
202.344.4704

Ronald M. Jacobs
rmjacobs@venable.com
202.344.8215

Michael A. Signorelli
masignorelli@venable.com
202.344.8050

Tara M. Sugiyama
tmsugiyama@venable.com
202.344.4363

E-COMMERCE, PRIVACY, AND MARKETING ATTORNEYS

Two of the "Top 25 Privacy Experts" by *Computerworld* 2007

"Winning particular plaudits" for "sophisticated enforcement work"– *Chambers and Partners*

Authors/editors of the forthcoming *BNA Portfolio on Privacy Law*

Recognized in the 2008 United States editions of *Chambers USA* and *Legal 500* for its outstanding data protection and privacy practice

"Among the nation's first privacy lawyers"– *Chambers and Partners*

1.888.VENABLE
www.Venable.com

In this Issue:

Congress returned to a short legislative calendar following the party conventions in Minneapolis and Denver. Given the limited time that Congress will be in session as a result of the elections, it will be difficult for further consideration of legislation that has been in the pipeline for the past year. While possible, it is unlikely that spyware, data security, Federal Trade Commission reauthorization, or other privacy and marketing related bills will advance prior to the November elections. It is possible that there could be additional activity in the Committees on these issues. The Senate Commerce Committee has indicated its intent to hold an additional hearing on ISP-based "behavioral advertising" this fall. Similarly, the House Energy and Commerce Committee may continue its inquiry into this area. The FTC also could provide further guidance to its proposed self-regulation for behavioral advertising.

This issue of the *Download* includes articles on the ongoing inquiry by the House Energy and Commerce Committee into Internet advertising and describes two new browsers that may provide technology solutions to these issues. Additionally, included is a summary of the FTC's recently issued Final Rule Amendments to the Telemarketing Sales Rule that prohibits telemarketing calls using prerecorded messages without prior express consent even where there exists an established business relationship. Finally, an International roundup indicates a busy fall for cross-border data flow programs.

© VENABLE 2008

HEARD ON THE HILL

House Committee Examines Internet Advertising Practices

The House Committee on Energy and Commerce on August 1, 2008 requested 33 cable, phone, and Internet companies to respond to a series of questions regarding the trend of companies tailoring Internet advertising based upon consumers' Internet search, surfing, or other use. Congressional hearings in the spring and summer focused on tracking of consumer web interactions performed by Internet service providers (ISP) for ad targeting purposes. The Committee letter, signed by Representatives Joe Barton (R-TX), John Dingell (D-MI), Ed Markey (D-MA), and Cliff Stearns (R-FL), asked the companies to state the nature and extent to which they have engaged in such practices and the impact it could have on consumer privacy. Below is a summary of the responses to the Committee.

Few Companies Testing "Deep Packet Inspection" Technology

In response to the Committee's letter, the majority of the companies indicated that they had not tailored or facilitated the tailoring of Internet advertising based on consumers' Internet use. A small handful of companies indicated that they had tested tailored Internet advertising. Of these companies, all but one explicitly stated that they had tested the technology in partnership with NebuAd for a limited period of time with a discrete set of customers. Charter Communications, a company that had received a prior letter from the Committee directing it not to engage in such practices, indicated that it had considered initiating a limited pilot of NebuAd's enhanced advertising, but ultimately chose not to move forward with the pilot.

Significant Consumer Privacy Protections Built into Targeted Internet Advertising

A common theme among the responses to the Committee was that companies already provide significant consumer protection and support providing customers with robust notice and choice. For instance, Cable One stated it supported first obtaining affirmative consent via an "opt-in" option from customers to use the technology, and then providing them with the continuous ability to opt out of having their information used for behavioral advertising purposes.

Charter Communications indicated in its comments that NebuAd's system itself is designed to honor consumer privacy. Charter Communications comments explained that NebuAd's system contains both contractual and technical measures built in to avoid tracking or serving of advertisements based on Internet visits related to medical information, racial or ethnic origins, religious beliefs, adult content, or content of a sexual nature. Others indicated that that the NebuAd technology does not use, track, or store personally identifiable information, such as a first and last name, physical street address, email address, telephone number, social security number, or information from password-protected sites (e.g., HTTPS traffic).

© VENABLE 2008

Expansion of Inquiry Beyond DPI

What began as a focus on ISP based behavioral advertising during the Committee's July 17, 2008 hearing on privacy implications of using the technology for Internet advertising services was expanded by the Committee's August 1, 2008 letter. The letter broadened the scope of the inquiry to include an examination of technologies beyond ISP behavioral targeting to practices by Internet companies that involve tailoring Internet advertising based upon consumers' Internet use. In response to the Committee's letter, companies described other technologies and practices used to perform behavioral advertising.

AT&T's comments noted for example, that ISP based behavioral targeting is not the most prevalent technology used by companies to track a consumer's overall web search and web browsing activities. AT&T asserted that advertising-network operators "have the ability to observe a user's entire web browsing experience at a granular level, including all URLs visited, all searches, and actual page-views. Techniques include the ad network 'dropping' third-party tracking 'cookies' on a consumer's computer to capture consumer visits to any one of thousands of unrelated websites; embedding software on PCs; or automatically downloading applications that – unbeknownst to the consumer – log the consumer's full session of browsing activity."[1]

Google, Microsoft, and Yahoo! each commented on the value of Internet advertising created through non-ISP behavioral tracking practices. Google indicated that its services deliver advertising products to hundreds of thousands of small businesses and other companies around the world. Microsoft explained that its service delivers personalized advertisements through its own properties and the sites of advertising partners. Yahoo! stated that it operates display and sponsored search advertising platforms that provide customized advertising to the company's users.

MARKETPLACE

Two New Internet Browsers Introduced

In the last several weeks, two new Web browsers were announced. Microsoft on August 27, 2008 released Internet Explorer 8, beta 2. On September 2, 2008, Google released its new beta Web browser, Google Chrome. Both browsers provide new tools that permit consumers to choose how information about their online activity is collected, stored, or shared.

IE 8, beta 2

Microsoft's new Internet Explorer ("IE 8") permits consumers to browse the Internet without leaving "any trace of specific web browsing activity." The suite of features provided in IE 8 limit browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser. IE 8 include the following features:

- **Delete Browsing History** – this feature allows a user to delete browsing history while preserving data (e.g. cookies and temporary Internet files) and preferences on web sites that have been saved in the user's favorites.

AT&T Letter, Aug. 13, 2008, p.2.

© VENABLE 2008

- **InPrivate browsing –** this feature allows a user to browse the Internet without IE 8 retaining browser history or storing files, such as cookies, in the user's temporary files. When viewing the Web using InPrivate, IE 8 will not store new history entries, form data, passwords, addresses typed into the address bar, queries entered into the search box, or visited links. A user can activate this feature by selecting the 'InPrivate' button on a new tab page within the browser.

- **InPrivate blocking –** this feature permits users to allow or block third-party content on web pages they visit. The tool is designed to block third-party content that appears across web sites visited by a user. Content delivered directly from the web page visited by a user is not blocked.

- **InPrivate Subscriptions –** this feature allows a user to subscribe to third party "allow or block lists." The subscription list subscribed to will either block or allow access to third party content while a user activates InPrivate Browsing.

These features, if used by consumers, which effect how data concerning users may be collected and maintained, will impact the Internet experience of users, web publishers, content providers, and third party networks. For example, Web publishers' content provided by third parties, such as local weather and news, or recalling a user's preferences, and relevant advertisement delivered by third party networks may not appear.

Microsoft has offered recommendations on how third-party content providers can reduce the risk of their content being blocked through the InPrivate feature. Microsoft suggests that web publishers and third-party content providers enter arrangements in one of two ways by which the content appears as first-party content. One option is for the web-publisher to host the content of their partners within their domain. The other option is for the web publisher to alias partner servers to sub domains of the web publisher. These suggestions may prove helpful for web application providers, provided the parties are able to reconcile business and branding objectives, but it may not assist network advertisers. Such entities can also join InPrivate subscriptions lists that may be developed in the future that will allow content by trusted third parties.

Google Chrome

Google's new web browser also includes a feature that allows consumers to browse the Internet anonymously. This feature, called "Incognito," allows users to browse the web without the web pages and files downloaded being logged in a user's browsing and download histories. When a user closes an "Incognito" window, no new cookies from that session will be stored. This feature limits the Chrome browser from storing information about the site the user visited. It does allow the visited web site to make a record of the user's visit. The files saved to a user's computer will remain there after the Chrome browser is closed.

Google announced on September 8, 2008, that it has modified its log retention policy. Google stated that in response to regulatory concerns it will anonymize IP addresses on their server logs after nine months. IP addresses were previously anonymized after eighteen months.

© VENABLE 2008

AROUND THE AGENCIES:

FTC Amends Telemarketing Sales Rule to Prohibit Prerecorded Messages

Nearly two years after it issued proposed rules, the Federal Trade Commission ("FTC") has adopted final amendments to the Telemarketing Sales Rule ("TSR") dealing with prerecorded messages and abandoned calls. These amendments make the rules governing prerecorded messages significantly more restrictive than the current rules.

I. Prerecorded Messages

The amended rules prohibit any "outbound telephone call that delivers a prerecorded message" unless (1) the seller has an express written agreement from the recipient of the call to receive prerecorded messages; (2) the message includes certain disclosures within two seconds after the completion of the called party's greeting; and (3) the caller provides an opt-out mechanism (using either voice or keypad) to allow the person to place him- or herself on the seller's company-specific do-not-call list.

The provision requiring an express agreement does not become effective until September 1, 2009. Until that time, the FTC will allow prerecorded messages to those with whom the caller has an established business relationship ("EBR"). The provisions requiring the disclosures and the opt-out mechanism become effective December 1, 2008 (even for EBR prerecorded calls).

Written Agreement to Receive Calls: The agreement to receive prerecorded messages must be in writing. In addition, the agreement must meet these requirements:

1. The seller must obtain the consumer's agreement to receive prerecorded message calls after it makes a clear and conspicuous disclosure that the purpose of the agreement is to authorize the seller to place prerecorded calls to the consumer;
2. The seller must obtain the agreement without requiring, directly or indirectly, that the agreement be executed as a condition of purchasing any good or service;
3. The agreement must evidence the willingness of the consumer to receive calls that deliver prerecorded messages by or on behalf of a specific seller; and
4. The agreement must include the consumer's telephone number and signature.

The rules allow the signature to be obtained electronically or digitally as long as it is otherwise recognized as a valid signature under applicable federal or state contract law.

The requirement to obtain an agreement applies only to calls to "induce the purchase of goods or services." It does not apply to outbound calls that seek a charitable contribution, "information only" calls (e.g., calls to notify persons that their flight has been cancelled), or business-to-business calls.

© VENABLE 2008

Required Disclosures in Prerecorded Messages: All prerecorded messages that induce the purchase of a good or service must, within two seconds after the completed greeting of the person called, disclose the following:

1. The identity of the seller;
2. That the purpose of the call is to sell goods or services;
3. The nature of the goods or services; and
4. If a prize promotion is offered, that no purchase or payment is necessary to be able to win a prize or participate in a prize promotion and that any purchase or payment will not increase the person's chances of winning.

Prerecorded calls that induce a charitable contribution from a nonprofit charitable organization's member or previous donor must include the following disclosures within two seconds after the completed greeting of the person called:

1. The identity of the charitable organization on behalf of which the request is being made; and
2. That the purpose of the call is to solicit a charitable contribution.

Opt-Out Mechanism in Prerecorded Messages: For prerecorded calls that either induce the purchase of goods or services or that induce a charitable contribution, the call must include, immediately after the required disclosures, an opt-out mechanism. If the call could be answered in person by a consumer then the person called must be able to use an automated interactive voice and/or keypress-activated opt-out mechanism to assert a company-specific do-not-call request. If the call could be answered by an answering machine or voicemail service, then it must allow the person called to use a toll-free telephone number to add him or herself to the company-specific do-not-call list.

The prerecorded message rules do not apply to any outbound call from a covered entity or its business associate that delivers a prerecorded healthcare message, as defined under HIPAA privacy rules found at 45 C.F.R. § 160.103.

II. Abandoned Calls

The FTC also amended the method callers must use to measure the abandonment rate. This part of the rule becomes effective on October 1, 2008, and provides that abandoned calls shall be "measured over the duration of a single calling campaign, if less than 30 days, or separately over each successive 30-day period or portion thereof that the campaign continues." The TSR previously required the abandonment rate to be measured on a per-day per-campaign basis.

© VENABLE 2008

OVERSEAS

International Roundup – Busy Fall for Cross-Border Data Flow Programs

Safe Harbor Program

The European Union Safe Harbor Program is growing at a faster pace than ever before. During the first seven years of its existence, the Program grew at a pace of less than 200 organizations per year. By comparison, during the first half of 2008, more than 200 new organizations registered with the Program.

As the number of organizations participating in the Program exceeds 1600, and searching the public registry for certified companies becomes increasingly unwieldy, the U.S. Department of Commerce has developed a certification mark allowing companies to demonstrate visibly their compliance with the Safe Harbor standards to European consumers and business partners. Companies will be able to display the certification mark on their web sites, similar to the manner in which companies display their Better Business Bureau or TRUSTe certification marks. More information is available at www.export.gov/safeharbor.

The certification mark initiative comes as the Commerce Department prepares to launch a pilot project that, like the European Union Safe Harbor Program, would allow U.S. organizations receiving personal data across international borders to certify their compliance with the privacy principles developed by the 21-member Asia Pacific Economic Cooperation, with enforcement provided by the Federal Trade Commission. The pilot project could culminate in the adoption of a self-certifying framework for APEC in 2009.

European Union

The European Union's Article 29 Working Party is expected to release further information this month on two of the mechanisms for satisfying the Data Protection Directive when transferring personal data outside of the EU. First, the Working Party is expected to publish a new alternative set of controller-to-processor model contract clauses. Second, the Article 29 Working Party is expected to release additional information on implementing Binding Corporate Rules, including the status of mutual recognition of BCRs by the data protection authorities of the EU member countries.

Meeting of Privacy Commissioners in Strasbourg

The 30th International Conference of Data Protection and Privacy Commissioners will convene next month in Strasbourg, France. This conference, held annually, brings together the privacy commissioners and data protection authorities of 78 countries for three days for a mix of public and private sessions. The theme for this year's conference is "Protecting Privacy in a Borderless World." Additional information is available at www.privacyconference2008.org

© VENABLE 2008

Announcements

We are delighted to welcome Thomas Cohn to Venable's team. Tom brings 17 years of Federal Trade Commission experience to one of the nation's leading law firms handling FTC and state attorney general investigations. Tom's experience includes investigations and enforcement actions in the privacy, data security, and marketing areas. He has served in Washington, DC, as Counselor to the Director of the Bureau of Consumer Protection and, more recently, in New York as Director of the FTC's Northeast Regional Office. Tom Cohn is resident in Venable's New York office.

Venable office locations

BALTIMORE, MD
750 E. PRATT STREET
NINTH FLOOR
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

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

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

TOWSON, MD
210 ALLEGHENY AVENUE
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

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

WASHINGTON, DC
575 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

The *Download* is published by the law firm of Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations. You're 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

© VENABLE 2008