Extracted from *Law360*:

Takeaways From The Hulu Privacy Case

Law360, New York (April 30, 2014, 1:56 PM ET) -- Any company that hosts videos on websites and uses analytics or includes a "Like" button or other social plug-in should pay very close attention to the April 29 decision in In re Hulu Privacy Litigation. In the Hulu case, the named plaintiffs allege that Hulu wrongfully disclosed their video viewing selections and "personally identifiable information" to third parties comScore and Facebook in violation of the Video Privacy Protection Act. The VPPA prohibits disclosures of personally identifiable information that is defined as including information that identifies a specific individual as having requested or obtained video materials or services.

Background Regarding the Summary Judgment Motion

On Feb. 27, 2014, the Northern District of California heard oral argument on Hulu's motion for summary judgment. In that motion, the Northern District of California characterized Hulu's arguments as including assertions that Hulu did not violate the VPPA because "(I) it disclosed only anonymous user IDs and never linked the user IDs to identifying data such as a person's name or address; (II) it did not disclose the information 'knowingly' and thus is not liable; and (III) Hulu users who are Facebook users consented to the disclosures because Facebook's terms of use permitted disclosure." Order Granting In Part And Denying In Part Hulu's Motion For Summary Judgment (Comscore And Facebook) April 28, 2014 ("Order").

The Purported comScore Class Was Dismissed on Summary Judgment as Unique Identifiers Are Held to Be Insufficient to Identify a Specific Person

In their motion for class certification (also before the court), the plaintiffs defined the comScore class as follows:

comScore Disclosure Class

All persons residing in the United States and its territories who, from March 4, 2011 through November 8, 2012, were registered users of hulu.com (including, but not limited to, paying subscribers, also known as Hulu Plus subscribers) and requested and/or obtained video materials and/or services on hulu.com during the Class Period.

Order at p. 3.

The plaintiffs argued that the comScore disclosures involved disclosures of two Web beacons that contained Hulu Unique Identifiers (HUID) — i.e., randomly assigned numbers for user devices.

The first Web beacon came from "watch pages" or pages where video was actually viewed on Hulu.com. The Web beacons sent to comScore for watch pages included the following elements: (1) a HUID; (2) a GUID (browser identifier); (3) Ad ID; and (4) the video name or title from the URL.[1]

The second Web beacon that went to comScore was for registered users on Hulu. On or about March 12, 2009, Hulu began providing each registered user with a profile webpage. The first and last name the user provided during registration appeared on the page and in the page title that was captured in the Web beacon along with the HUID, but no video viewing information was disclosed. Because the HUID was in the URL of users' profile page, Magistrate Judge Laurel Beeler stated that "comScore had the 'key' to locating users' associated profiles that revealed the names the users provided when they signed up for Hulu." Order at p. 6.

For their part, the plaintiffs argued that comScore had the ability to compile the two Web beacons into one database — tracking users by name, unique identifier and video views, and using a comScore ID that linked the two Web beacons together.

Hulu argued that it did not disclose PII because HUID numbers are not personally identifying. And, further,

the reports it received from comScore were not PII because they never identified a user by name and instead presented the data in an "aggregated and generalized basis, without reference even to User IDs." Order at p. 5.

In deciding these issues, the Northern District court stated the "issue is whether the information transmitted to comScore is "information which identifies a person as having requested or obtained specific video materials." 18 U.S.C.§ 2710(a)(3). "If it is, then the transmission violates the VPPA." Order at p. 10. In so ruling, the court acknowledged that what was at issue under these facts was whether "Hulu's disclosures here (unique numeric identifications tied to video watching) are PII under the VPPA." Order at p. 12.

The statute states that "[t]he term 'personally identifiable information' ["PII"] includes information which identifies a person as having requested or obtained specific video materials or services." Id. § 2710(a)(3). After reviewing the legislative history, the court concluded that "[t]he plain language of the statute suggests, and the Senate Report confirms, that the statute protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched." Order at p. 12.

The court relied on a series of authorities to support the conclusion that serial numbers or unique identifiers alone are not PII under the VPPA. The court seemed most persuaded by the Tenth Circuit's decision in Pruitt v. Comcast Cable Holdings LLC, 100 F. App'x 713, 716-17 (10th Cir. 2004). In Pruitt, the Tenth Circuit considered whether Comcast disclosed PII by issuing its old cable converter boxes to new customers without deleting the pay-per-view purchase histories stored in the cable boxes.

The Tenth Circuit held that it did not because the converter boxes did not contain "the name, address or any information regarding the customer." Instead, they contained a hexadecimal code that "enables Comcast to identify a customer's viewing habits by connecting the coded information with its billing management system." The Cable Act has been held to be analogous to the VPPA. Order at p. 16.

Relying on Pruitt and similar authority, Magistrate Judge Beeler concluded that the three comScore disclosures did not amount to violations of the VPPA. First, disclosure of the watch page and the HUID did not "suggest any linking of a specific, identified person and his video habits." Order at p. 18. Second, Hulu's coding of its watch pages to cause the user's Web browser to send comScore a "comScore ID" that was unique to each registered user and allowed comScore to gather significant behavioral data regarding users off of the Hulu.com website did not violate the VPPA because, according to the court, there is a "VPPA violation only if that tracking necessarily reveals an identified person and his video watching." Order at p. 19.

Despite ruling in Hulu's favor, the court rejected Hulu's argument that the VPPA prohibits only disclosures of video viewing that identify a person by their "actual name." The court stated "[t]hat position paints too bright a line. One could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table. The statute does not require a name." Order at p. 17. The court further stated:

In sum, the statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person.

Id.

Alleged Facebook Disclosures Using the "Like" Button Were Held to Be Potentially Personally Identifiable Information Under the VPPA

With regard to the Facebook functionality, the court explained the technology as follows:

Certain information was transmitted from hulu.com to Facebook via the Facebook "Like" button through June 7, 2012 (when Hulu stopped including the video title in the watch page URL).

Order at p. 7.

Magistrate Judge Beeler acknowledged that when a "user's browser executes th[e] code [on the Hulu webpage]" — i.e., when a user visits the Hulu webpage containing the Facebook "Like" button:

[T]he request included a 'referer URL' value (the URL of the page from which the request issued) in the request headers and the query string. That is how Facebook knows where to send code for the Like button so that it can be downloaded and used. Until June 7, 2012, the URL for each watch page included the title of the video displayed on that watch page. The IP address of the Hulu registered user's computer also was sent to Facebook.

Order at p. 7-8.

The court further described the technology as follows: "[b]ecause the URL of the watch page specified the title of the video during the period from April 21, 2010, to June 7, 2012, Facebook would know the title of the video being viewed." Order at p. 9

Facebook also received certain cookies. "Hulu sent code and information to load the Facebook Like button that included the following: (1) the watch page with the video name; (2) generally the user's IP address; (2) the datr cookie identifying the browser; (3) the lu cookie that identified the previous Facebook user using the browser to log into Facebook (with a life of two years); and (4) the c_user cookie for any user who logged into Facebook using the default setting in the past four weeks." Order at p. 20.

Despite the fact that there was no evidence that Facebook did anything with those cookies, the plaintiffs' expert opined that "Hulu's disclosure to Facebook of cookie identifiers set by Facebook's domain enabled Facebook to link information identifying the user and the user's video choices to other information about the particular user." Order at p. 8.

With regard to the Facebook cookies, the court concluded:

the lu and the c_user cookies—sent with the datr cookie at the same time the watch page loaded with the video name—together reveal information about what the Hulu user watched and who the Hulu user is on Facebook. It also is a Hulu-initiated transmission of information.

Order at p. 20.

The court was not persuaded by Hulu's argument that this was based upon the functionality of the Internet. As the court stated, the plaintiffs introduced evidence that it was "straightforward" to build a webpage that did not cause those disclosures. "Put another way, it was not necessary to send the 'Facebook user' cookies, and they were sent because Hulu chose to include the Like button on watch pages." Order at p. 21.

Further, the court was not impressed by Hulu's argument that "… the data sent to Facebook is not necessarily PII because it reveals only the last Facebook user to log in to that computer or use that browser." The court concluded instead that this was a "fact issue" that could not be resolved on summary judgment. Order at p. 22.

The court also recognized that the VPPA only prohibits knowing disclosures of PII. "If Hulu did not know that it was transmitting both an identifier and the person's video watching information, then there is no violation of the VPPA. By contrast, if it did know what it was transmitting, then (depending on the facts) there might be a VPPA violation." Order at p. 23

Hulu may not have been able to read Facebook's cookies, but if it knew what they contained and knew that it was transmitting PII—that is, information that identifies a person as having requested or obtained specific video materials or services, 18 U.S.C. § 2710(a)(3)—then Hulu is liable under the VPPA. In sum, arguing that transmitting cookies is just the normal way that webpages and the Like button load is not enough to negate knowledge or show the absence of evidence about knowledge.

Order at p. 24 (emphasis added).

The court cited to emails in the record reflecting Hulu may have been aware of the attendant disclosures associated with the Like button and concluded:

[t]hese points suggest purposefulness about allowing the use of vendor cookies to track Hulu users. They also suggest that Hulu knew that using beacon technology to disclose user data could result in identification of actual users, and it recognized the VPPA implications.

Order at p. 25.

The court distinguished the comScore Web beacons, where two separate Web beacons would have to be linked by comScore, to the Facebook cookies, where the Facebook user ID was contained in the same cookie as the video titles.

The court recognized, however, that "[t]he analysis would be different if the Facebook cookies were sent when a user pressed the Like button. Information transmitted as a necessary part of a user's decision to share his views about his videos with his friends on Facebook would not support a VPPA violation." Order at p. 21.

The Court Concluded There Were Triable Issues of Fact Regarding Consent

The VPPA permits disclosure to any consumer with the consumer's informed, written consent. During the class period that predated amendments to the VPPA's consent provisions, consent required "the informed, written consent of the consumer given at the time the disclosure is sought." 18 U.S.C. § 2710(b)(2)(B) (pre-January 2013 amendments).

The court concluded that to support consent, Hulu relied upon Facebook's current policies as of September 2013, but did not tie those back to the class period for the 2010-2012 time period. "Hulu cites only Facebook's current policies and information on its Help Center in September 2013." Order at p. 26.

The court also was not persuaded that it could decide as a matter of law that consent was obtained based upon Hulu's arguments concerning the enforceability of "click-wrap agreements." Effective January 2013, consent can now be obtained electronically, in a separate legal document, for up to two years in advance. 18 USC § 2710(b)(2)(B)(i)-(ii).

The Court Concluded That the VPPA's Exemption of Disclosures Incident to the Ordinary Course of Business Did Not Apply to the comScore and Facebook Claims

The VPPA permits disclosures that are "incident to the ordinary course of business." The statute narrowly defines "incident to the ordinary course of business" to mean "only debt collection activities, order fulfillment, request processing, and the transfer of ownership." 18 USC § 2710(a)(2).

On Hulu's August 2012 motion to dismiss, Magistrate Judge Beeler held that the "ordinary course of business" exception was not a defense that could be decided on motion to dismiss:

Whatever the merits are to Hulu's contentions that it uses the challenged services to deliver targeted advertisements to its users, Plaintiffs alleged unauthorized tracking of Plaintiffs' data (including video content information). The court cannot resolve this factual issue in a motion to dismiss. Put another way, as pled, the claim survives a Rule 12(b)(6) motion.

In re Hulu Privacy Litig., 2012 U.S. Dist. LEXIS 112916 * 21 (N.D. Cal. Aug. 10, 2012).

Although, the question of the applicability of this defense in this case was left open, Magistrate Judge Beeler suggested strongly that she did not believe that the exemption would ultimately apply on summary judgment:

Market research and web analytics are not in the ordinary course of Hulu's business of delivering video content to consumers.

Id. *20.

Although the Northern District had previously left open the question of whether the disclosures to Facebook and comScore were "incident to the ordinary course of business," the parties did not brief this issue on summary judgment. Hulu referred only briefly to this question in a single footnote. Even though the scope of the "incident to the ordinary course of business" defense was not at issue on summary judgment, the court reached the question in its order.

Magistrate Judge Beeler concluded sua sponte on summary judgment that:

The transmissions here are not incident to Hulu's "ordinary course of business" as that term is defined in the statute. See 8/10/12 Order, ECF No. 68 at 9-10. For example, as discussed below, Hulu initiated the transmission of the Facebook ID cookies before any action by Facebook, and the cookies were not necessary to Hulu's order fulfillment and request processing. Tracking start-stop times for advertising might require identification of an anonymized user ID, but the comScore UID was not part of orders processing. Indeed, the point of the ID cookies was to track Hulu users' activities. The other exceptions do not apply.

Order at p. 11-12.

In so holding, the court reasoned that:

The transmission of the cookies to load the Like button was not necessary to Hulu's business and instead apparently was a benefit for Facebook to leverage its platform and gain information about its users (presumably through the deployment of the Like Button). (The same is true of the comScore UID, which allowed comScore to track and gain information about users.) Hulu wrote and installed the code that integrated the Like button on the watch pages, and it transmitted the Facebook ID cookies when it sent the request to Facebook to load the Like button.

Order at p. 25.

Recommendations for Companies in Light of Hulu

The Hulu litigation has been ongoing since 2011. To potentially avoid exposure, companies should focus on compliance best practices with regard to videos on their websites. Compliance legal teams, IT and marketing should have a thorough understanding of the information they are collecting and disclosing to third-party service providers as well as the timing for those disclosures. Further, companies should explore methods for obtaining consent under the statute.

The risks are significant — i.e., $2,500 per violation and (in many cases) millions of alleged violations, sometimes per day, depending upon the website or online service.

1. Best Practices For Compliance: comScore/Analytic Company Disclosures

Magistrate Judge Beeler left open the question of whether unique identifiers could still be PII depending upon context. Because comScore Web beacons were not linked and there was no evidence that comScore actually linked them, there was not context to find PII under these circumstances.

- For compliance and to avoid the risk that ID number disclosures could constitute PII, companies should:
    - Determine whether the disclosures to analytic companies contain, within one cookie, a unique identifier, video viewing and some other potentially identifying information equivalent to a name.
    - Adequately train staff and employees to avoid communications between analytic companies and staff that could imply knowledge that non-PII data (e.g., unique identifiers) will be linked with PII.

- Review existing agreements with analytic companies to determine whether agreements authorize linking of datasets.

2. Best Practices for Compliance: Facebook Disclosures

- Consider all sites that contain Facebook "Like" buttons and assess how the Facebook "Like" button configuration occurs for each site.

- Determine whether Facebook cookies are being deployed and disclosed at the time the user clicks the "Like" button or simply by visiting the webpage. Magistrate Beeler specifically contemplated a scenario in which a user could provide consent by hitting a "Like" button. In the Hulu case, the deployment of cookies (containing the Facebook user ID and video viewing) before a user hit the "Like" button gave rise to a triable issue of fact.

—By Dominique Shelton, Kim Chemerinsky and Sheila Shah, Alston & Bird LLP

Dominique Shelton is a litigation partner and Kim Chemerinsky and Sheila Shah are associates in Alston & Bird's Los Angeles office.

[1] Specifically, until June 7, 2012, the URL (uniform resource locator, meaning the web address) of Hulu's watch pages, included the name of the video on that page (e.g., http://www.hulu.com/watch/426520/saturday-night-live-the-californians-thanksgiving).