Hulu Video Privacy Protection Act Summary Judgment Ruling in the N.D. of California Emphasizes Importance of Knowing What Data Companies Are Collecting And Sharing When Consumers Watch Video Online

On Monday, April 28, 2014, the Northern District of California in *In Re: Hulu Privacy Litigation*, No. 3:11-cv-03764-LB (M.J. Laurel Beeler), issued a summary judgment opinion under the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, that underscores the challenges and risks companies can face in sharing user video behavior information with third parties through web beacons and other online tools.

The VPPA, enacted originally in the wake of Judge Bork's Supreme Court confirmation hearings, generally prohibits videotape service providers from knowingly disclosing personally identifiable information ("PII") of a consumer, including a consumer's video viewing history, to a third party. The VPPA also provides for a private right of action and permits a court to award statutory damages of at least $2500 per violation and attorneys' fees, which has led plaintiffs' attorneys to seek to apply it to the online world.

The class action brought against Hulu is an example. Hulu is an online video service that allows users to watch video on-demand through "watch pages." The plaintiffs generally alleged that the "beacon" technology used by Hulu's analytics vendor, comScore, also transmitted PII to comScore and that the placement of a "Like" button on a watch page resulted in Facebook unlawfully receiving PII too. Hulu moved for summary judgment, arguing that (i) it only disclosed anonymous user IDs, not PII; (ii) if the information was PII, it did not "knowingly" disclose it under the VPPA; and (iii) Facebook users consented to the disclosure.

The comScore Disclosures

The information comScore received through beacons on Hulu's watch page included 1) the Hulu user's unique identification number ("Hulu User ID"); 2) an alphanumeric string Hulu used to differentiate between web browsers; 3) the Hulu "Ad ID" identifying a particular advertisement being played; 4) the name of the program or video being watched; and 5) the unique comScore user ID ("comScore UID") that linked the user and video choice information to other information it gained about the same user when the user visited other sites where comScore collects data.

The court, following a number of cases to consider the issue, held that an anonymous unique identifier, without more, is not PII under the VPPA. Applying that holding to the information that Hulu provided to comScore, the court held that providing Hulu User IDs along with information about the videos watched, by itself, was not a violation of the VPPA. The court reasoned that the VPPA requires "identifying the viewers and their video choices" and that a unique identifier, without more, does not violate the VPPA.

The plaintiffs argued that comScore could use the unique Hulu User ID to access the Hulu profile page of a user and then capture the user's first and last name from the profile page. However, because the plaintiffs failed to show that comScore actually did that, the court granted Hulu summary judgment. In doing so, the court looked at the evidence "very practically" and noted that while comScore "doubtless collects as much evidence as it can about what webpages Hulu users visit" and there may be "substantial tracking that reveals a lot of information about a person," it held a VPPA violation occurs "only if that tracking necessarily reveals an identified person and his video watching."

The Facebook Disclosures

The court found the disclosures to Facebook to be more problematic. Hulu's placement of the Facebook Like button on a watch page meant that, in addition to the URL web address of the Hulu watch page (which at the time also contained the video name), four sets of data were automatically sent to Facebook via Facebook's cookies: 1) the user's IP address; 2) the datr cookie identifying the browsers; 3) the lu cookie that identified the previous Facebook user using the browser to log into Facebook; and 4) the c_user cookie for any user who logged into Facebook using the default setting in the past four weeks. All this information was sent with the loading of the Hulu watch page, without the user having to click the Like button.

The court noted several key differences between the data made available to comScore and the data made available to Facebook. Because the lu and the c_user cookies transmitted Facebook IDs, the court found that the information identified the Hulu user. By including in Hulu's single transmission to Facebook the video name and the Facebook user cookies, the court found "the link between the user and the video was more obvious." While strongly suggesting that that was enough to trigger the VPPA, the court held there was a material question of fact as to whether that information was sufficient to identify individual consumers.

The court also held there was an issue of material fact as to whether Hulu "knowingly" disclosed this information to Facebook, as required by the knowledge element of the VPPA. Since inclusion of the Like button was an optional choice, and not necessary for the function of Hulu's watch pages, the court thought more information was needed. It offered that "it might be dispositive if Facebook could not auto-authenticate a user when the Like button loaded" but also that, even if Hulu was itself unable to read Facebook's cookies, if Hulu "knew what they contained and knew that it was transmitting PII . . . then Hulu is liable under the VPPA."

Hulu also argued that Facebook users had consented to disclosure of their information through Facebook's "click-wrap agreements." The VPPA previously required, through early January 2013 (which includes the period at issue in the lawsuit), that the "informed, written consent of the consumer [be] given at the time the disclosure is sought."[1] The court stated that it had no evidence that, at the time in question, this kind of consent was sought, and so rejected the argument.

The *Hulu* decision highlights the importance of being aware of what user information is tracked through a company's online properties, by whom, and how. The Northern District of California court appears to be willing to impose liability under the VPAA for the information included and transmitted in cookies placed by third parties, even if the company sending those cookies cannot read or control them. The potential for that liability underscores the importance of adopting and implementing "privacy by design" principles in all aspects of online development and thinking through user consent issues carefully. For more information, feel free to contact Jim DeGraw, Debbie Gersh, Tim McCrystal, Dave McIntosh, Doug Meal, Mark Szpak, Michelle Visser or any other member of our leading privacy & data security practice team.

[1] The VPPA currently allows sharing of PII and video information to "any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that- (i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; (ii) at the election of the consumer- (I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." 18 U.S.C. 2710(b)(2)(B)