ALSTON&BIRD LLP

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

FEBUARY 27, 2014

Northern District of California to Decide in the *In re Hulu Privacy Litigation* Whether Disclosing Anonymized Data to a Web Analytics Company and Use of the Facebook "Like" Button Violate the Video Privacy Protection Act

Any company that has a website that (a) contains videos, (b) uses a third-party analytics company to maintain metrics on page views and/or (c) allows users to "like" videos on the site should pay very close attention to the *In re Hulu Privacy Litigation* pending in the United States District Court of Northern California. In that case, the plaintiffs are seeking statutory damages of $2,500 per violation for alleged video sharing in violation of the Video Privacy Protection Act (VPPA). As there are millions of views per day on the Hulu site, the alleged statutory damages could represent significant exposures.

As the practices that are being challenged in the Hulu case are so commonplace for websites, the case is being watched closely by businesses and could change the way many websites and mobile apps deliver streaming content.

By way of background, since July 2011, Hulu has vigorously defended a consumer class action, *In re Hulu Privacy Litigation*, Case No. 4:11-cv-03764 (N.D. Cal. 2011), in which the plaintiffs initially alleged that Hulu violated the VPPA by disclosing their video viewing selections and personal identification information to third parties such as Kissmetrics (an Ad Network), Scorecard (the research arm of comScore) and Google Analytics (companies that appear on many website's Ad Choices links). As discussed below, the plaintiffs have now dropped their claims concerning Google Analytics disclosures.

The VPPA prohibits disclosure of personally identifiable information (PII), including information identifying a person as requesting specific video material. 18 U.S.C. § 2710, *et seq*. The VPPA does not define PII directly, stating that it "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). This includes information shared with vendors, including subject matter categories. Some vendors argue that generic categories (e.g., "likes sports") are not PII.

Hulu has made several attempts to end the case through motions to dismiss and one motion for summary judgment on harm that was recently decided in December 2013. *See* Alston & Bird Client Alert, "2013 Ends with a Bang – Northern District of California Denies Hulu's Motion for Summary Judgment in Video Tracking Case." Most recently, on December 20, 2013, the court held that the plaintiffs need not demonstrate "actual injury" above and beyond the alleged unauthorized disclosure of their video viewing to third parties in order to maintain their VPPA claims. None of the attacks based upon standing or the lack of applicability of the VPPA have carried the day.

Before the court now is Hulu's final motion for summary judgment, which is based upon the contention that Hulu has not violated the VPPA because it did not disclose any PII or video viewing. Hulu filed this second motion for summary judgment on October 1, 2013; it focuses on three key arguments:

First, Hulu asserted that it has not violated the VPPA by disclosing anonymized user numbers to third-party analytics companies because this information is not "personally identifiable information." Specifically, Hulu contended that the VPPA prohibits disclosure of the user's name and video titles, and not the sort of anonymized data disclosed by Hulu. In response, the plaintiffs contended that the VPPA itself does not limit the definition of PII to "names," but even if the data disclosed by Hulu was "anonymized," comScore employees nevertheless could "reverse engineer" the data by searching for the names of Hulu users through users' Hulu profile pages.

Second, Hulu further contended that even if comScore or Facebook could "re-identify" the Hulu User IDs with names or other personal information, such data shared through the "like" button and Facebook's corresponding "datr" cookie is not visible to Hulu, and Hulu is not responsible for Facebook's use of this data. The plaintiffs responded that the VPPA statute does not contain a definition of PII that is limited to "names" and "video," but rather Section 2710(a)(3) of the VPPA defines PII as "information which identifies a person as having requested or obtained specific video materials or services" and that user IDs can be used to identify a person.

In opposition to Hulu's motion for summary judgment, the plaintiffs have narrowed their claims considerably to the following practices they contend constitute violations of the VPPA. The claims are nevertheless disturbing because many companies engage in the activities that form the basis of the plaintiffs' pared-back claims every day in connection with their website and mobile app operations. Specifically, the plaintiffs' opposition brief reveals challenges to the following practices:

- Hulu's disclosures of anonymized Hulu User IDs to comScore. The User IDs are numerical values that are assigned by Hulu to the browsers for users that visit the site. No names, email addresses or other identifying information is shared by Hulu with comScore.
- Hulu's use of the comScore beacon to provide information to comScore for its analytic purposes. The comScore "beacon" on the Hulu watch page includes four types of information: (1) the Hulu "User ID," (2) the GUID (string of numbers and letters that Hulu assigns at random to a web browser when a registered user logs into hulu.com), (3) the "Ad ID" (a unique number Hulu assigned to each advertisement shown) and (4) the name of the program (and any data regarding a video's season and episode number).

- Hulu's implementation of the Facebook "like" button plug-in that allegedly shares the referral URL, reflecting the web page that the user was visiting before navigating to Facebook through the like button.

- comScore's use of a unique ID for users. Hulu argues in its motion for summary judgment that it did not have access to comScore's proprietary UDID.

Following two motions to dismiss, class certification and a motion for summary judgment, the *Hulu* court has narrowed the focus of the litigation to a single claim, alleging that Hulu's data transmissions to third parties violated the VPPA, which prohibits a "video tape service provider" from transmitting personal identifying information of "consumers" (except for certain permissible disclosures). These are ubiquitous practices, undertaken by each and every corporation that maintains a website and shares data in order to analyze basic metrics about the website and its users.

At the hearing on February 27, 2014, Magistrate Judge Laurel Beeler observed that the disclosure of anonymized data is not enough to show a violation of the VPPA. A violation of the VPPA occurs only where a party discloses information specific to the individual, as well as information about the videos viewed by that individual. Thus, Judge Beeler asked the parties to point to specific facts to show the character of Hulu's disclosures in this case.

Judge Beeler further opined that Hulu's disclosures to Facebook through the "like" button seemed to present a markedly different scenario than Hulu's disclosures to comScore. Judge Beeler noted that "Facebook feels harder" because the Facebook ID may be more easily matched to the user's video viewing activities. Although early motions may lay out the limits of liability, it is difficult to determine based on the record at hand whether these disclosures were "knowing" and whether Hulu or Facebook has the "responsibility for coding."

The court pointed out that plaintiffs have argued that Hulu, and not Facebook, is responsible for the disclosure and use of information in connection with Facebook's "like" button. Hulu's counsel responded to this point, arguing that Hulu lacks any information whatsoever as to what Facebook does with the information it receives through the "like" button widget. When a user navigates to Facebook's webpage, Facebook loads a cookie for the "like" button, which is linked to the login user profile for the last person who signed into the site. All Hulu did was open the door for third parties to obtain this information. Thus, Hulu contended that it is not responsible for the disclosure of this information.

The court responded that Hulu's point appeared to provide stronger support for the plaintiffs' arguments regarding disclosures to comScore rather than Facebook. The court then asked for more information regarding application to the like button for Facebook. In doing so, the court noted that the disclosure of an anonymized code to a party that fully understands it, like Facebook, differs from the disclosure of this information to an analytics entity like comScore.

Magistrate Beeler stated that maybe her own knowledge of the digital world may prevent her from easily deciding the Facebook question, though she noted that she is into the "grains of the expert declarations" at this point to see what they establish or not establish. Nevertheless, the court suggested that it was not

inclined to accept Hulu's argument that the inquiry should end based on what was disclosed, i.e., only anonymized data: "Saving my Facebook ID to Facebook electronically is far more illuminating to Facebook than my name Laura Beeler." The court observed that just because some entities have the ability to correlate anonymized data does not mean that comScore does. In contrast, the court noted, "the Facebook ID is me." Magistrate Beeler analogized a Facebook user ID to a "photo ID."

Magistrate Beeler then posed a different question to the plaintiffs' counsel. She pointed out that while there may be privacy issues, we are just relying on the VPPA statute. And the key issue is whether there are any violations of that statute. The plaintiffs' counsel directed the court to a Hulu email, reflecting an exchange between Facebook and Hulu regarding VPPA compliance. The email noted that Facebook developers' guidelines placed onus on publishers. Thus, the plaintiffs argued that Hulu knew from day one that the like button had VPPA implications.

The court was not persuaded by the plaintiffs' contention that this email supported their claim of a VPPA violation. Instead, the court framed the legal question as whether the disclosure of the unique identifiers is the "equivalent" of a name.

In evaluating the comScore disclosure issue, the court asked the plaintiffs' counsel whether Hulu would say Hulu uses comScore for certain reasons. Plaintiffs' counsel responded that Hulu, during the class period, referred to comScore the first and last name and the user ID of Hulu account holders. Hulu responded that even the disclosure of a user's first and last name itself does not amount to a violation of the VPPA if that information is not tied to specific information of the user's video viewing activities.

Although the vast majority of the two-hour argument focused on Hulu's motion for summary judgment, the court afforded thirty minutes of limited argument regarding the certification of a "comScore disclosure class" and a "Facebook disclosure class." Magistrate Judge Beeler indicated that she had questions regarding the ascertainability of a Facebook class, asking how the court should address the ascertainability issue "[i]f I don't like the comScore theory and I like the Facebook theory better." Notably, Magistrate Judge Beeler did not raise any signification questions regarding the certification of a prospective comScore class, and posed no questions targeted to that class. This suggests that the court did not believe that Hulu violated the VPPA in its disclosures to comScore.

As to the certification of a "Facebook class," Hulu's attorneys focused on the point that enormously different factual issues made the proposed class not suitable for certification, e.g., individual class members who used ad-blocking or do-not-track mechanisms. The plaintiffs responded to this argument, contending that Hulu users could not view videos unless they enabled tracking mechanisms. Thus, the plaintiffs' attorneys claimed that the use of ad-blocking software or "do-not-track" software did not create individual issues to preclude class certification.

The court took the matter under submission, and it remains to be seen how the court will come out on the above issues. Our take-away from the hearing was that the court seemed to be focused on whether the disclosure of a Facebook ID was the equivalent of disclosing a user's name in connection with viewing information. The court announced its intention to delve further into the application of the facts to this

principle in order to reach a decision as to Hulu's motion for summary judgment, as well as the plaintiffs' motion for class certification. No matter the outcome, the court's decision in *Hulu* threatens to make VPPA litigation the next vehicle for plaintiffs' lawyers to seek what has been described as "annihilating damages" from companies who stream video on their websites and mobile applications.

Best Practices:

The VPPA was amended in December 2012 to allow video service providers to obtain consent electronically over the Internet for a two-year advance period with certain requirements. It requires a separate consent (outside of a terms of use and privacy policy). Section 2710(b)(2)(B) was amended to permit electronic consent. Video service providers can share information with the user's informed written consent that:

- is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;
- is at the election of the consumer;
- is given at the time the disclosure is sought or is given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and
- 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.

To minimize risks, companies should consider making efforts to obtain advance consent.

- Website operators should attempt to obtain consent before tracking a user's video viewing activities and sharing the same with third parties. They should implement ESIGN best practices for electronic consent over the Internet or via mobile devices. If they do not obtain consent, website operators should delete a visitor's PII if that visitor has not visited any of the company's "websites" (as that term is defined in the company's privacy policy) within the past 365 days.
- If a visitor opts out of receiving commercial emails or withdraws her consent to the sharing of her PII with third parties, the company should consider immediately decoupling the visitor's video viewing history from any other PII belonging to that visitor.
- If a website operator does not have the consumer's consent, it should only share visitors' PII with third parties in the following situations:
  - the disclosure is limited to the visitor's name and address; or
  - the disclosure is incident to the ordinary course of business. Note that the *Hulu* court has previously ruled that the ordinary course of business exemption to the VPPA is limited only to "debt collection activities, order fulfillment, request processing, and the transfer of ownership."

Companies should be aware of the current heightened litigation and regulatory enforcement environment around privacy and take care to prioritize compliance in their video practices.

Los Angeles Office
Dominique R. Shelton | 213.576.1170 | dominique.shelton@alston.com

Los Angeles Office
Kim Chemerinsky | 213.576.1079 | kim.chemerinsky@alston.com

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Megan K. Callahan
megan.callahan@alston.com
404.881.4283

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Stephanie B. Driggers
stephanie.driggers@alston.com
404.881.7163

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Kacy McCaffrey
kacy.mccaffrey@alston.com
404.881.4824

Todd S. McClelland
todd.mcclelland@alston.com
404.881.4789

Zachary Neal
zach.neal@alston.com
404.881.4968

Bruce Sarkisian
bruce.sarksian@alston.com
404.881.4935

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

Kim Kisabeth Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Claire L. Readhead
claire.readhead@alston.com
213.576.1181

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Nicholas Stamos
nick.stamos@alston.com
213.576.2515

Washington, D.C.

Edward Britan
edward.britan@alston.com
202.239.3364

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Paul G. Martino
paul.martino@alston.com
202.239.3439

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jeffrey R. Sural
jeff.sural@alston.com
202.239.3811

ALSTON&BIRD LLP

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213-576-1100
NEW YORK: 90 Park Avenue ■ 12th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 275 Middlefield Road ■ Suite 150 ■ Menlo Park, California, USA, 94025-4004 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333