May 1, 2014

Decision from Northern District of California Addresses Scope of VPPA Coverage in the Online Context

By D. Reed Freeman, Julie O'Neill and Patrick Bernhardt

In a much anticipated decision in the class action *In re Hulu Privacy Litigation*, U.S. Magistrate Judge Laurel Beeler of the U.S. District Court for the Northern District of California has shed new light on the meaning of "personally identifiable information" (PII) under the Video Privacy Protection Act (VPPA).[1] This has important implications for companies that host videos on their websites and integrate their services with social media companies or web analytics service providers.

The court held on summary judgment that the transmission to a third party of unique user IDs, *in and of themselves*, along with video viewing history, does not constitute disclosure of PII under the VPPA. In reaching its conclusion, the court distinguished between anonymous IDs that Hulu, LLC provided to the audience metrics company comScore, Inc. (which the court held were not PII) and a social networking service's user IDs that Hulu provided to the social networking service (as to which the court held there were material issues of fact with respect to whether they could permit the identification of specific persons and thus be PII). The court granted Hulu's motion for summary judgment with respect to the comScore disclosures but not with respect to the social networking service disclosures.

KEY POINTS

The court's decision shows that, when determining whether unique IDs associated with consumers' online video viewing history are PII regulated by the VPPA, context matters. In particular, companies that transmit such information should be aware of several key points:

- First, the decision declined to impose VPPA liability for the disclosure of unique user IDs associated with video viewing history, where such IDs did not identify specific persons and where the record revealed only a hypothetical ability to correlate unique user IDs to specific persons but no evidence that it actually happened.

[1] *In re Hulu Privacy Litigation*, No. C 11-03764 LB (N.D. Cal. filed Apr. 28, 2014) (Order Granting in Part and Denying in Part Hulu's Motion for Summary Judgment) ("Order").

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Daniel F. Muto (858) 720-7959
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Peter McLaughlin (212) 336-4290
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Ann Bevitt 44 20 7920 4041
Caroline Stakim 44 20 7920 4055
David Varney 44 20 7920 4058

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

- Second, the decision makes clear that companies should be mindful of the context in which they share unique user IDs with third parties, particularly with respect to whether the IDs permit the recipient or another party to identify specific persons, either directly or through information to which they already have access.

- Third, the decision highlights the potential danger for companies that integrate social media plug-ins or other functionality on web pages where consumers watch videos. Companies providing online video services should consider taking steps to ensure that: (1) cookies and other data transmitted to another entity, such as a user ID that is matched with the video provider's user ID for the same person, do not permit identification of specific individuals; and (2) video viewing history is not shared unintentionally, such as through a referrer URL that is transmitted during a standard browser request.

- Fourth, the decision highlights other important questions of fact that may exist when evaluating VPPA exposure, including whether the disclosing party had knowledge of the disclosure and whether the consumer consented to it.

BACKGROUND

With limited exceptions, the VPPA imposes liability—including liquidated damages of up to $2,500 per incident—on a video tape service provider that knowingly discloses, to any person, PII concerning any consumer of the video tape service provider.[2] Liability extends to companies that provide online video services, such as Hulu, and the definition of PII includes "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[3]

In this case, the plaintiffs alleged that Hulu wrongfully disclosed its users' video viewing history to comScore and a social networking service. comScore had provided Hulu with audience metric data about Hulu's users, and the social networking service had provided social networking features through placement of its "Like" button on Hulu's video watch pages. Each company received different data from Hulu during the delivery of its services. Among other data, comScore received unique numerical Hulu User IDs and comScore User IDs, while the social networking service had access to its own first-party cookies containing its own unique user IDs. Each company also received the title of the video watched, either as a parameter in a set of data transmitted or in the referrer URL of the page on which the user viewed the video.

ASSESSING THE LINK BETWEEN USER IDS AND SPECIFIC PERSONS

In its decision, the court addressed three different disclosures by Hulu: (1) the disclosure to comScore of watch pages and Hulu User IDs; (2) the disclosure to comScore of the comScore User ID cookies; and (3) the disclosure to the social networking service of watch pages and the social networking service's cookies.

The key issue for the court was whether the disclosures of the video titles were tied to specific identified persons, such that they constituted prohibited disclosures of PII under the VPPA. The court stated that "the statute, the legislative history, and the case law do not require a name, [but] instead require the identification of a specific person tied to a specific transaction . . . ."[4] **Providing further explanation, the court stated 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*."**[5] **In other words, context matters insofar as the circumstances link the unique user IDs to specific persons.**

[2] 18 U.S.C. § 2710(b)(1).

[3] 18 U.S.C. § 2710(a)(3).

[4] Order at 17.

[5] *Id.* (emphasis added).

In applying this reasoning, the court held that Hulu's disclosure to comScore of watch pages and Hulu User IDs did not constitute disclosure of PII: despite the fact that comScore could have used the Hulu User IDs to access Hulu users' profile pages and obtain their names, there was no evidence that it did so, and there was thus no disclosure of PII for purposes of the VPPA.[6]

The court next addressed Hulu's disclosure to comScore of the comScore User ID cookies. **The court explained that, although the comScore User IDs permitted comScore to conduct "substantial tracking that reveals a lot of information about a person," the disclosure did not violate the VPPA because the tracking did not reveal "an identified person and his video watching."**[7]

On the other hand, the court suggested that disclosure of the social networking service's own, first-party user IDs to the social networking service itself, together with video viewing history, may constitute disclosure of PII under the VPPA. The court noted that "[t]he Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion."[8] In addition, **the court emphasized that "a Facebook user—even one using a nickname—generally is an identified person on a social network platform" and that "[the Facebook User ID] identifies the Hulu user's actual identity on Facebook."**[9] Therefore, the court denied Hulu's motion for summary judgment with respect to its disclosures to the social networking service.

The decision with respect to the social networking service highlights the risk posed by integrations with social media companies on websites that host video services. Such integrations may cause a cookie or other data to be sent from a user's browser without any affirmative action by the user, which could permit the social media company to identify a specific person and his or her video watch history—and thus trigger VPPA liability, although the court declined to make a decision on this aspect at this stage of the proceedings. In practical terms, this risk means that companies providing online video services should take steps to ensure that: (1) cookies and other data transmitted to another entity, such as a user ID that is matched with the video provider's user ID for the same person, do not permit identification of specific individuals; and (2) video viewing history is not shared unintentionally, such as through a referrer URL that is transmitted during a standard browser request.

OTHER POTENTIAL LIMITATIONS UNDER THE VPPA: "KNOWING" DISCLOSURE AND USER CONSENT

The court ruled that material issues of fact remained regarding whether Hulu disclosed the social networking service's user IDs knowingly and without user consent. The court stated that "[o]ther cases involving violations of privacy statutes show that in the context of a disclosure of private information, 'knowingly' means consciousness of transmitting the private information. It does not mean merely transmitting the code."[10] Thus, the court stated that "if [Hulu] knew what [the social networking service's cookies] contained and knew that it was transmitting PII . . . then Hulu is liable under the VPPA."[11] The court did not, however, grant summary judgment to Hulu based simply on the fact that Hulu's servers could not read the social networking service's cookies. Rather, the court held that other evidence may show that Hulu knew that the

[6] *Id.* at 18.

[7] *Id.* at 19 (emphasis added).

[8] *Id.* at 21.

[9] *Id.* (emphasis added).

[10] *Id.* at 23.

[11] *Id.* at 24.

social networking service was receiving its own first-party user IDs within its cookies and was reading them together with video viewing history.

Finally, the court also denied Hulu's motion for summary judgment with respect to whether consumers had given consent to any disclosures through their acceptance of the social networking service's privacy policy or whether such "consent," if found, was sufficient under the VPPA.

CONCLUSION

In light of the court's decision, companies that—without affected individuals' VPPA-compliant consent—disclose any type of identifier, together with video viewing history, to any other person or company should pay very close attention to exactly what information they transmit and whether it could be used by the recipient to identify specific individuals.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.