UNITED STATES DISTRICT COURT

Northern District of California

San Francisco Division

IN RE: HULU PRIVACY LITIGATION

No. C 11-03764 LB

ORDER GRANTING IN PART AND DENYING IN PART HULU'S MOTION FOR SUMMARY JUDGMENT (COMSCORE AND FACEBOOK)

_____/

[ECF No. 125-4]

INTRODUCTION

In this putative class action, viewers of Hulu's on-line video content allege that Hulu wrongfully disclosed their video viewing selections and personal identification information to third parties such as metrics companies (meaning, companies that track data) and social networks, in violation of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710. Second Amended Consolidated Class Action Complaint ("SAC"), ECF No. 83 at 7-8.[1] In their class certification motion, Plaintiffs limit the third parties to comScore, a metrics company that analyzes Hulu's viewing audience and provides reports that Hulu uses to get media content and sell advertising, and the social network Facebook. *See* Motion For Class Certification, ECF No. 111.

The Act prohibits a "video tape service provider" from knowingly disclosing "personally

[1] Citations are to the Electronic Case File ("ECF") with pin cites to the electronic page number at the top of the document.

UNITED STATES DISTRICT COURT
For the Northern District of California

identifiable information of a consumer of the provider" to third parties except under identified exceptions that do not apply here. *See* 18 U.S.C. § 2710. "The term 'personally identifiable information' includes information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider." *Id.* § 2710(a)(3).

Hulu argues that it 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. Motion for Summary Judgment, ECF No. 125-4 at 1-2.

The court grants the summary judgment motion as to the comScore disclosures and denies it as to the Facebook disclosures. The comScore disclosures were anonymous disclosures that hypothetically could have been linked to video watching. That is not enough to establish a VPPA violation. As to the Facebook disclosures, there are material issues of fact about whether the disclosure of the video name was tied to an identified Facebook user such that it was a prohibited disclosure under the VPPA. In addition, the record is not developed enough for the court to determine as a matter of law whether Hulu knowingly disclosed information or whether Hulu users consented to the disclosures.

STATEMENT

I. THE PARTIES AND THE PROPOSED CLASSES

Hulu provides on-demand, online access to television shows, movies, and other pre-recorded video content from networks and studios through its website, www.hulu.com. SAC ¶¶ 1, 17. It offers a free service at hulu.com that allows users to watch video content on their computers. *See* Joint Statement of Undisputed Facts ("JSUF") #1. It also offers a paid service called "Hulu Plus" that has more content and allows viewers to watch Hulu content on other devices such as tablets and smart phones. Yang Decl. ¶¶ 2, 6.

Plaintiffs Joseph Garvey, Sandra Peralta, Paul Torre, Joshua Wymyczak, and Evan Zampella each are registered Hulu users. *See* SAC ¶¶ 1-6. Sandra Peralta, Evan Zampella, and Paul Torre became paying Hulu Plus subscribers in July 2010, June 2011, and July 2012, respectively. *See id.*

¶¶ 3-4, 6, 34. The SAC alleges that Hulu wrongfully disclosed Plaintiffs' video viewing selections and "personally identifiable information" to third parties comScore and Facebook, all in violation of the VPPA. *See id.* ¶¶ 51-63; Motion for Class Certification, ECF No. 111.

Plaintiffs ask the court to certify two classes: the comScore disclosure class and the Facebook disclosure class. *See* Class Cert. Motion, ECF No. 111 at 2. The class definition are 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.
>
> ***Facebook Disclosure Class***
>
> All persons residing in the United States and its territories who, from April 21, 2010 through June 7, 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.

II. HOW HULU WORKS

Hulu pays license fees to studios, networks, and other rights holders to obtain the video content that it offers to its users. *See* Yang Decl, ¶ 10, ECF No. 12-6. Hulu allows users to register for a free Hulu account. *See* JSUF #1. A Hulu user does not need to register for a Hulu account to watch videos on hulu.com using a personal computer. *See* Yang Decl. ¶ 4. To register for a Hulu account, the user enters a first and last name, birth date, gender, and an email address. JSUF #1. Users are not required to provide their legal first and last name during registration. JSUF #2. In fact, Plaintiff Joseph Garvey registered for his Hulu account in a name other than his legal name. *See* JSUF #3. Hulu does not verify the accuracy of the identifying information but stores it in a secure location. Yang Decl.¶ 6. To register for Hulu Plus, the user must provide the same information as a registered Hulu user, payment information, and a billing address. Yang Decl. ¶ 7. Hulu assigned each new registered Hulu user a "User ID," which is a unique numerical identifier of at least seven digits (*e.g.*, 50253776). JSUF #6; s*ee* Tom Dep., Carpenter Decl. Ex. 7, ECF No. 157-11 at 37:9-38:12.

The videos on hulu.com are displayed on a video player that appears on a webpage. Hulu calls these webpages "watch pages." *See* Yang Decl. ¶ 3; *see* JSUF #24. Hulu wrote and deployed the

code for its watch pages. Tom Dep., Carpenter Decl. Ex. 7, ECF No. 157-11, at 108:23-109:8, 175:9-16; Wu Dep., Carpenter Decl. Ex. 2, ECF No. 157-6, at 80-84. The code downloaded to registered Hulu users' browsers when they visited a watch page so that the browser could display the requested web page or video content. Tom Depo., Carpenter Decl. Ex. 7, ECF No. 157-11 at 112:19-113:5. As described in more detail below, the code also allowed information to be transmitted to comScore and Facebook. 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). JSUF #24 (the number in the URL, here 426520, is the video ID).

On or about March 12, 2009, Hulu began providing each registered user with a profile web page. JSUF #9. The first and last name the user provided during registration appears on the page and in the page title. JSUF #10. Hulu did not allow registered users to decline to share their first and last names on their public profile pages. Until August 1, 2011, a user's profile page URL included the user's unencrypted Hulu User ID. JSUF #12. An example is http://www.hulu.com/profiles/u/[User ID], where "[User ID]" is the Hulu User ID. *Id.* After August 1, 2011, the Hulu User ID was encrypted. JSUF #13. An example is http://www.hulu.com/profiles/u/wxu2RqZLhrBtVjYKEC_R4. *Id.* Hulu did not provide a separate search function (for example, through a search box) to allow a user to use a Hulu User ID to find the profile page of another user. JSUF #11. On May 30, 2013, Hulu discontinued the user profile pages. JSUF #14.

Hulu makes money from advertising revenue and from monthly premiums paid by Hulu Plus members. Yang Decl., ¶ 11. Its main source of income is advertising revenue. *Id.* Advertisers pay Hulu to run commercials at periodic breaks during video playback. *Id.* ¶ 12. Advertisers pay based on how many times an ad is viewed. *Id.* ¶ 13. Hulu thus gathers information (or metrics) about its "audience size." *Id.* Advertisers require verified metrics, which means that Hulu needs to hire trusted metrics companies. *Id.* comScore is one of those companies. *Id.* ¶ 14.

comScore collects metrics on digital media consumption using its Unified Digital Measurement methodology. Carpenter Decl. Ex. 22, ECF No. 155-27 (comScore press release cross-referencing its 2012 SEC Form 10-K and its Q1 2013 SEC Form 10-Q), Ex. 32, ECF No. 155-32 (Addendum to

Hulu-comScore contract). As of 2013, comScore captured 1.5 trillion digital interactions each month and had more than 2000 clients. *Id.* Ex. 22; *see Harris v. comScore, Inc.*, 292 F.R.D. 579, 581 (N.D. Ill. 2013) (describing comScore's business).

III. HOW HULU INTERACTS WITH COMSCORE

According to Hulu, comScore gives it "reports containing metrics regarding the size of the audience for programming on hulu.com," and Hulu uses the reports to obtain programming and sell advertising. Yang Decl., ECF No. 125-6, ¶ 14. The reports never identify a user by name and instead present the data in an "aggregated and generalized basis, without reference even to User IDs." *Id.* Hulu uses the comScore metrics to show "other content owners . . . that the Hulu audience is a desirable outlet for their programming, and to convince advertisers of the value of reaching Hulu's audience." *Id.* Mr. Yang said in his deposition that he did not know why Hulu sent individual comScore user IDs (see below) if comScore provided only aggregate information, and he did not know whether comScore provided other reports with individual-level data. *See* Yang Dep., ECF No. 125-3 at 102-04, 108-11.

comScore uses "beacon" technology to track audience metrics. *Id.* ¶ 15. A "beacon" is triggered by defined events during the playing of a video such as when the video starts, when the advertisement starts, when it ends, and when the video re-starts. *Id.* The beacon, when triggered by an event, directs the user's browser to send a piece of HTTP programming code to comScore that contains certain defined "parameters" (meaning, pieces of data or information). *Id.* ¶ 16.

From March 27, 2010 through November 8, 2012, when a user watched a video on hulu.com, Hulu, which wrote the code to transmit the data, transmitted information to comScore by using a comScore "beacon" on the Hulu watch page. JSUF #4-5. The beacon included four pieces of information: (1) the Hulu user's unique numerical Hulu User ID; (2) the "GUID," a long alphanumeric string[2] that Hulu used to differentiate between web browsers and that Hulu assigned at random to a browser when it accessed hulu.com; (3) the Hulu "Ad ID," a unique six-digit number that identifies only the advertisement; and (4) the name of the program and any season or episode

[2] An example of a "GUID" is 767DE299767B4E577B787B40B5123C30. JSUF #7.

number. JSUF #5-8. Hulu suspended sending the Hulu User ID on November 8, 2012. JSUF #4.

comScore's possession of the Hulu User ID allowed it to connect all information that was tied to that Hulu User ID. *See* Calandrino Decl., ECF No. 160-5, ¶¶ 30, 33-34, 47. Because the Hulu User ID was in the URL of users' profile page, comScore had the "key" to locating users' associated profiles that revealed the names the users provided when they signed up for Hulu. *Id.* ¶¶ 35-37. The user profile pages were all in a standard format: http://www.hulu.com/profiles/u/[User ID]. As discussed above, the watch page contained the video title. The argument is that comScore could easily access the profile page and see the user's first and last names (or at least the names that the users gave when registering) and connect that to the user's viewing information. For Hulu Plus members, presumably the names would correspond to their billing and payment information (and thus likely reflected the users' true names).

The code Hulu wrote and included in each watch page also caused a unique numeric or alphanumeric "comScore UID" for each registered user to be communicated from the registered user's browser to comScore. *See* Wills Decl., ECF No. 160-6, ¶¶ 36-37; JSUF#15, 17. The comScore UID is stored in a comScore cookie and identifies the specific copy of the web browser. JSUF #15-17. The comScore cookie enabled comScore to link the identified user and video choice information to other information it gained about the same user when the user visited websites where comScore collects data. Calandrino Decl., ECF No. 160-5, ¶¶ 48-56; Wills Decl. ECF No. 160-6, ¶ 36.

For context, a cookie is a file on a user's computer. Wu Decl., ECF No. 125-7, ¶ 13. Cookies contain information that identifies the domain name of the webserver that wrote the cookie (e.g., hulu.com, comScore.com, or facebook.com). *Id.* ¶ 18. Cookies have information about the user's interaction with a website. *Id.* Examples include how the website should be displayed, how many times a user has visited the website, what pages he visited, and authentication information. *Id.* ¶ 13.

Each web browser on a computer (e.g., Internet Explorer or Chrome) stores the cookies that are created during a user's use of the browser in a folder on the user's computer that is unique to that browser. *Id.* ¶ 14. When a user types a website address into the browser, the browser sends (a) a request to load the page to the webserver for that website address and (b) any cookies that are

associated with the website (such as the cookies on the user's computer for "hulu.com" or "comScore.com"). *Id.* ¶ 15. The remote website server returns the requested page and can update the cookies or write new ones. *Id.* The only servers that can access a particular cookie are those associated with the domain that wrote the cookie. *Id.* ¶¶ 18, 21. That means that Hulu can read only hulu.com cookies, and it cannot read comScore.com cookies or facebook.com cookies.

That being said, according to Plaintiffs, Hulu hosts its vendors' JavaScript code on Hulu's domain so that when Hulu's web pages execute the vendor code, a vendor such as comScore obtains information through cookies that are set by hulu.com. *See* Carpenter Decl. Ex. 10, ECF No. 158-2 at HULU_GAR231508 (vendors need to set cookies on hulu.com for tracking; example given was google analytics); *id.* Ex 11, ECF No. 158-3 at HULU_GAR 093686 (email from Hulu to Google; hulu user goes to hulu.com to watch a video; user's browser calls invite_media (presumably where content is); cookies from there will be passed on to Google; Google can set cookies on the user). More specifically as to comScore, Hulu's documents have examples of code that sets comScore identifiers, including its UID and UIDR cookies. *See id.* Exs. 11-15, ECF Nos. 158-3 to 158-7.

IV. HOW HULU INTERACTS WITH FACEBOOK

Facebook collects information and processes content "shared by its users," and it provides that information to marketers when it sells them its products (identified as "Facebook Ads," "Facebook Ad System," and "Ad Analytics and Facebook Insights"). *See* Carpenter Decl. Ex. 8, ECF No. 157-12 (Facebook 2012 SEC Form 10-K). Facebook shares its members' information with marketers so that marketers can target their ad campaigns. *See id.* Marketers can "specify the types of users they want to reach based on information that users choose to share." *Id.* Advertisement revenue is how Facebook makes money. *See id.*

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). JSUF #18. During this time period, Hulu included a Facebook Like button on each hulu.com watch page. JSUF #18-19. Hulu wrote code for its watch pages that included code for where the "Like" button should be located on the page and where (from facebook.com) to obtain the code that loads and operates the button. JSUF #20. When the user's browser executed this code, the browser sent the

request to Facebook to load the Like button. JSUF #21. The request included a "referer URL" value (the URL of the page from which the request issued) in the request headers and the query string. JSUF #21. That is how Facebook knows where to send code for the Like button so that it can be downloaded and used. Wu Decl. ¶¶ 16, 20. Until June 7, 2012, the URL for each watch page included the title of the video displayed on that watch page. *See* JSUF #18. The IP address of the Hulu registered user's computer also was sent to Facebook (although there are scenarios when the IP address might not be that of the users but instead of a proxy or intermediary). *See* Tom Depo., Carpenter Decl. Ex. 7, ECF No. 157-11 at 190:23-192:12.

Facebook also received the following cookies associated with the facebook.com domain: (1) a "datr" cookie, which identifies the browser; (2) a "lu" cookie, which "can contain the Facebook user ID [e.g., 286xxxx1] of the previous Facebook user to log in to Facebook via the browser and has a lifetime of 'two years;'" and (3) if the user had logged into Facebook using default settings within the previous four weeks, a "c_user" cookie, which contains the logged-in user's Facebook user ID. JSUF #22; Calandrino Decl. ¶ 71. Hulu did not send Facebook the Hulu User ID or the Hulu user's name when the user's browser executed the code to load the Like button. JSUF #23.

No evidence has been introduced that Facebook took any actions with the cookies described above. JSUF #25. That being said, Plaintiffs' expert opines 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. *See* Calandrino Decl., ECF No. 160-5, ¶¶ 57-81. In common web browsers, visiting a website out of Facebook's control will not result in the communication of information to Facebook absent a decision (directly or indirectly) by the party controlling the website to send information. *Id.* ¶ 57. It is straightforward to develop a web page that "yields no communication with Facebook." *Id*. When a Hulu watch page loaded with the Facebook Like button, the page prompted a user's web browser to transmit the watch page URL and Facebook cookies to Facebook-controlled servers. *Id.* ¶ 58. This happened with the initial Hulu-prompted request from the user's browser to Facebook before the receipt of any information from Facebook. *Id.* ¶ 59. Because 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. *Id.* ¶ 61. The c_user cookie would give the name of the currently-logged in Facebook user. *Id.* ¶ 66. The lu cookie might too. *Id.* ¶ 71. A user is logged out of Facebook by default after closing the browser, but Facebook also provides users with an option to remain logged in after closing the browser. *Id.* ¶¶ 72-73. The lu cookie clears after a user selects Facebook's log-out option. *Id.* ¶ 74.

ANALYSIS

I. SUMMARY JUDGMENT

The court must grant a motion for summary judgment if the movant shows that there is no genuine dispute as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). Material facts are those that may affect the outcome of the case. *Anderson*, 477 U.S. at 248. A dispute about a material fact is genuine if there is sufficient evidence for a reasonable jury to return a verdict for the non-moving party. *Id.* at 248-49.

The party moving for summary judgment has the initial burden of informing the court of the basis for the motion and identifying those portions of the pleadings, depositions, answers to interrogatories, admissions, or affidavits that demonstrate the absence of a triable issue of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). To meet its burden, "the moving party must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial." *Nissan Fire & Marine Ins. Co., Ltd. v. Fritz Companies, Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000); *see Devereaux v. Abbey*, 263 F.3d 1070, 1076 (9th Cir. 2001) ("When the nonmoving party has the burden of proof at trial, the moving party need only point out 'that there is an absence of evidence to support the nonmoving party's case.'") (quoting *Celotex*, 477 U.S. at 325).

If the moving party meets its initial burden, the burden shifts to the non-moving party, which must go beyond the pleadings and submit admissible evidence supporting its claims or defenses and showing a genuine issue for trial. *See* Fed. R. Civ. P. 56(e); *Celotex*, 477 U.S. at 324; *Nissan Fire*, 210 F.3d at 1103; *Devereaux*, 263 F.3d at 1076. If the non-moving party does not produce evidence

to show a genuine issue of material fact, the moving party is entitled to summary judgment. *See Celotex*, 477 U.S. at 323.

In ruling on a motion for summary judgment, inferences drawn from the underlying facts are viewed in the light most favorable to the non-moving party. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

II. THE VIDEO PRIVACY PROTECTION ACT AND DISCLOSURES OF USER IDS

The VPPA is titled "Wrongful disclosure of video tape rental or sales records." 18 U.S.C. § 2710. It "'protect[s] certain personal information of an individual who rents [or otherwise obtains] video materials from disclosure.'" *See Dikes v. Borough of Runnemede*, 936 F. Supp. 235, 238 (D.N.J. 1996) (quoting S. Rep. 100-599, 2d Sess. at 16 (1988)). The protected information is "information which identifies a person as having requested or obtained specific video materials." 18 U.S.C. § 2710(a)(3).

"Aggrieved" persons may sue for knowing disclosures of information in violation of the statute. *See* 18 U.S.C. § 2710(b)-(c). Under the statute, a "court may award – (A) actual damages but not less than liquidated damages in an amount of $2,500; (B) punitive damages; (C) reasonable attorneys' fees and other litigation costs reasonably incurred; and (D) such other preliminary and equitable relief as the court determines to be appropriate." 28 U.S.C. §§ 2710(c)(2).

Plaintiffs purport to represent a class of "aggrieved persons." As consumers of Hulu's video content, they sue Hulu for transmitting their identifying information and the videos they watched to comScore and Facebook. The issue is whether the information transmitted to comScore and Facebook 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. *See id.* & 2710(b).

The next part of this order has three sections: A, B, and C. Section A analyzes the plain language of the statute and the legislative history and concludes that disclosed information must identify a specific person and tie that person to video content that the person watched in order to violate the VPPA. Section B examines whether there are triable issues of fact about whether the information transmitted to comScore and Facebook identified the watcher specifically enough to

establish a violation of the VPPA. Section B also addresses Hulu's argument that any disclosures were not "knowing." Section C addresses Hulu's argument that Facebook users consented to the disclosures.

A. The VPPA Prohibits Disclosures That Ties Specific People to the Videos They Watch

The VPPA prohibits a "***videotape service provider***" from (1) knowingly disclosing "to any person" (2) "***personally identifiable information***" concerning any "***consumer***" of such provider. *See* 18 U.S.C. § 2710(b) (emphasis added to identify terms to be defined).

A "***video tape service provider***" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710 (a)(4). The court previously held that Hulu was a "video tape service provider" within the meaning of the act. *See* 8/10/12 Order, ECF No. 68 at 7-9.

A "***consumer***" is "any renter, purchaser, or subscriber of goods or services from a video tape service provider." 28 U.S.C. § 2710(a)(1). The court previously held that Plaintiffs were consumers within the meaning of the Act. *See* 8/10/12 Order, ECF No. 68 at 11-12.

"The 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).

The VPPA allows certain disclosures including the following: (1) disclosures to the consumer; (2) disclosures to any person with the informed, written consent of the consumer given at the time the disclosure is sought;[3] (3) disclosures to law enforcement; or (4) disclosures that are "incident to the ordinary course of business," defined as "debt collection activities, order fulfillment, request processing, and the transfer of ownership." 28 U.S.C. § 2710(a)(2) & (b)(2). 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

[3] Congress amended the VPPA effective January 20, 2013. The amended statute, which does not apply here, broadens the consumer consent provisions. *See* 18 U.S.C. § 2710(b)(2) (2013).

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.

The issue is whether Hulu's disclosures here (unique numeric identifications tied to video watching) are PII under the VPPA. The statute's plain language prohibits disclosure of information that "identifies a person" as having (in the Hulu context) viewed specific video content. 28 U.S.C. § 2710(a)(3). It does not say "identify by name" and thus plainly encompasses other means of identifying a person. Indeed, PII is not given one definition: "the term . . . *includes* information which identifies a person. . . ." *Id.* That being said, considering the ordinary meaning of the plain language of the statute, the language supports the conclusion that the disclosure must be pegged to an identifiable person (as opposed to an anonymous person). The statute's plain language is ambiguous about whether it covers unique anonymous user IDs such as the Hulu ID. The court thus turns to the legislative history.

Congress's impetus for passing the VPPA was a newspaper's obtaining a list of video tapes that Supreme Court nominee and D.C. Circuit Judge Robert Bork rented from his local video store and then publishing an article about his viewing preferences. *See Dikes*, 936 F. Supp. at 238 (citing S. Rep. 100-599, 2d Sess. at 5). The Senate Report shows the legislature's concern with disclosures linked to particular, identified individuals. It states that VPPA's purpose was "[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials." S. Rep. 100-599, at 2 (1988). As Senator Leahy explained,

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read . . . . In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch. . . . I think that is wrong, I think that really is Big Brother, and I think it is something that we have to guard against.

Id. at *5-6. Senator Leahy also expressed concern about sophisticated information-tracking:

> [T]he trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance. These 'information pools' create privacy interests that directly affect the ability of people to express their opinions, to join in association with others and to enjoy the freedom and independence that the Constitution was established to safeguard.

> The bill prohibits video stores from disclosing "personally identifiable information" – information that links the customer or patron to particular materials or services. In the event of an unauthorized disclosure, an individual may bring a civil action for damages.

Id. at *7. The Senate Report includes an section-by-section analysis of the VPPA that elaborates on the statutory definition of personally-identifiable information:

> The term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape services provider. Unlike the other definitions in this subsection, paragraph (a)(3) uses the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information.
> . . .
>
> This definition makes clear that personally identifiable information is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider. The bill does not restrict the disclosure of information other than personally identifiable information. Thus, for example, a video tape service provider is not prohibited from responding to a law enforcement agent's inquiry as to whether a person patronized a video tape service provider at a particular time or on a particular date.

See id. at *11-12.

The 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. *See id.* at *7.

B. The Disclosures to comScore and Facebook

The issue then is whether the disclosures here are merely an anonymized ID or whether they are closer to linking identified persons to the videos they watched. A summary of the alleged disclosures is as follows:

1. Disclosure to comScore of Watch Page and Hulu User ID. The disclosure to comScore is of a "watch page" URL web address containing the video name and the Hulu user's unique seven-digit Hulu User ID. The ID also appeared in unencrypted form in the URL web address for the user's profile page in the standard format http://www.hulu.com/profiles/u/[User ID]. The profile page also listed the user's name (or at least the first and last name used to register with Hulu). This meant that comScore could access the profile page and see the user's first and last names.

2. Disclosure to comScore of the comScore UID (User ID) Cookie. Hulu sent comScore a "comScore ID" that was unique to each registered user. This allowed comScore to link the identified user and the user's video choices with information that comScore gathered from other websites that the same user visited. *See* Calandrino Decl. ¶¶ 48-56, ECF No. 160-5; Wills Decl. ¶ 36, ECF No. 160-6 at 10.

3. Disclosure to Facebook of Watch Page and Transmission of Facebook Cookies to Facebook. These disclosures included unique identifiers that sometimes included the user's IP address and sometimes contained the user's Facebook ID. Because the URL web address had the video name, Facebook could see its users and what they were watching.

Hulu argues that it is not liable for these three disclosures because it never combined or linked the user IDs to identifying data such as a person's name or address. Motion, ECF No. 125-4 at 7. It characterizes Plaintiffs' comScore case as "the theoretical possibility that comScore *could* have used the anonymous ID . . . to find the user's name." *Id.* at 8. It characterizes the Facebook case as "plaintiffs' evidence does not show that Facebook was gathering the actual name of its users from Hulu pages" and "there is no evidence that Facebook ever linked the anonymized identifier to a person's name, or to the title of a video that person watched." It concludes that the disclosure of the information here (even if linked to a specific video) is not a violation of the VPPA.

No case has addressed directly the issues raised by Plaintiffs: the disclosure of their unique identifiers and the videos they are watching. Most cases involve identified customers linked to the videos they watch. *See, e.g., Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1159 (W.D. Wash. 2010) (specific customer purchasers); *Mollett v. Netflix*, No. 5:11-CV-01629-EJD, 2012 WL 3731542 (N.D. Cal. Aug. 17, 2012) (Plaintiffs were viewers who watched Netflix videos through a "Netflix Ready Device" such as a game console, DVD player, or Internet television; Netflix's procedures required only a one-time password during the initial set-up; family members could see what Plaintiffs had watched; no VPPA violation because the disclosure was to consumers who thereafter were responsible for limiting access to their devices). Few cases even address unique anonymous IDs.

One case that does is *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 262 (S.D.N.Y. 2008).

Hulu cites it for the proposition that a unique, anonymous ID is not identifying information under the VPPA. Motion ECF No. 125-4 at 17. The case involved a discovery dispute in a copyright case brought by Viacom against YouTube. *Viacom*, 253 F.R.D. at 262. Viacom wanted YouTube's "logging" database that contained, "for each instance a video is watched, the unique 'login ID' of the user who watched it, the time when the user started to watch the video, the internet protocol address for other devices connected to the internet use to identify the user's computer . . . , and the identifier for the video." *Id.* at 261. YouTube argued that the VPPA barred it from disclosing the information. *Id.* at 262. What was at issue, however, was not the users' identities. Instead, because the case was a copyright case against YouTube, what mattered was the number of times the users viewed particular videos. *Id.* YouTube "did not refute that the login ID is an anonymous pseudonym that users create for themselves when they sign up with YouTube which *without more* cannot identify specific individuals." *Id.* at 262 (emphasis added). The court dismissed YouTube's privacy concerns as speculative and ordered discovery. *Id.*

That result makes sense: the case was about discovery to establish copyright damages, not consumers' identities. The consumer identities were not relevant. Indeed, Viacom issued a press release that the parties would anonymize the data before disclosure to address YouTube users' privacy concerns. *See* Carpenter Decl. Ex. 21, ECF No. 156-21. Also, the decision does not provide enough of a factual context to determine whether the user IDs in *Viacom* identified a person or were anonymized. The case's holding is relevant only to the extent that it recognizes that unique anonymous IDs do not necessarily identify people.

Another case that addressed unique anonymous IDs was *Lahr v. NTSB*, a Freedom of Information Act ("FOIA") case. *See* 453 F. Supp. 2d 1153, 1183 (C.D. Cal. 2006), *rev'd in part on other grounds*, 569 F.3d 969 (9th Cir. 2009). The *Lahr* court held that witness identification numbers alone did not disclose private information or allow access to the witnesses. *See id.* The FOIA applicant challenged the government's refusal to produce records relating to the investigation of an airplane that exploded in mid-air. The court applied the balancing test under the applicable FOIA exemption and held that the public interest in disclosure outweighed the government's objection that disclosing witness identification numbers would harm the witnesses' "interest in not

being subjected to unofficial questioning . . . and in avoiding annoyance or harassment in their . . . private lives." *Id.* at 1177, 1183-84. That holding was grounded on the government's "fail[ure] to explain how the disclosure of witness identification numbers, alone, could provide access to these individuals or any personally identifying information about them. Furthermore, the identification numbers are not personal information of a nature ordinarily protected by the courts under [the FOIA exemption], such as social security numbers or personnel records." *Id.* at 1183. Again, this decision supports only the conclusion that personally-identifiable information requires more than a unique anonymous ID.

Hulu cites a third unpublished case from the 10th Circuit that addresses the scope of PII under the Cable Act. *See Pruitt v. Comcast Cable Holdings, LLC*, 100 F. App'x 713, 716 (10th Cir. 2004). The Cable Act is a 1984 Act that establishes a scheme for the protection of personally-identifiable information regarding cable subscribers. *See* 47 U.S.C. § 551. Courts hold that the VPPA is analogous to the Cable Act. *See Parker v. Time Warner Entm't Co.*, No. 98 CV 4265(ERK), 1999 WL 1132463, at *9 (E.D.N.Y. Nov. 8, 1999). Like the VPPA, the Cable Act prohibits disclosure to third parties. The issue in *Pruitt* was whether Comcast disclosed PII by issuing the appellants' old cable converter boxes to new customers without deleting the pay-per-view purchase histories stored in the cable boxes. 1999 WL 1132463, at *9. The court held that it did not because the converter boxes did not contain "the name, address or any information regarding the customer." *Id.* 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." *Id.* The district court noted that "the converter box code – without more – provides nothing but a series of numbers." *Id.* The Tenth Circuit agreed, explaining:

> Without the information in the billing or management system one cannot connect the unit address with a specific customer; without the billing information, even Comcast would be unable to identify which individual household was associated with the raw data in the converter box. Consequently, it is the billing system that holds the key to obtaining personally identifiable information, not the converter box.

Pruitt, 100 F. App'x at 716. *Pruitt* stands for the proposition that an anonymous, unique ID *without more* does not constitute PII. But it also suggests that if an anonymous, unique ID were disclosed to a person who could understand it, that might constitute PII.

Hulu nonetheless argues that the disclosure has to be the person's actual name. Motion, ECF No. 125-4 at 18. That 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. It defines PII as a term that "includes information which identifies a person." 18 U.S.C. § 2710(a)(3). The legislative history shows Congress used the word "includes" when it defined PII to establish a minimum, but not exclusive, definition. *See* S. Rep. 100-599, at *11-12. It is information that "identifies a particular person as having engaged in a specific transaction with a video tape service provider" by retaining or obtaining specific video materials or services. *Id.* at *12; 18 U.S.C. § 2710(a)(3). It does not require identification by a name necessarily. One can be identified in many ways: by a picture, by pointing, by an employee number, by the station or office or cubicle where one works, by telling someone what "that person" rented. 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.

Hulu's other cited cases do not change this result. For example, it cites *Low v. LinkedIn Corp.* for the proposition that transmitting anonymous cookies is not a transmission of private information merely because the receiving party could "de-anonymize" the plaintiff's identity. *See* 900 F. Supp. 2d 1010 (N.D. Cal. 2012). The *Low* plaintiffs sued LinkedIn for transmitting their browsing histories (including their LinkedIn user IDs) to advertising and marketing companies. *See* 900 F. Supp. 2d at 1016-18. The privacy interest arose under the California Constitution, which requires a legally-protected privacy interest, a reasonable expectation of privacy under the circumstances, and conduct that amounts to a serious invasion of the protected interest. *Id.* at 1023. The court noted that the transmission of code was not the "'serious invasion' of a protected property interest" that the Constitution protected. *Id.* at 1024. The case does not alter the conclusion that a unique anonymized ID could be PII if other evidence renders it the equivalent of identifying a specific person.

Hulu's other cases similarly support only the conclusion that anonymous identification data

alone is not PII. *See, e.g., Millennium TGA, Inc. v. Comcast Cable Commc'ns, LLC*, 286 F.R.D. 8, 15-16 (D.D.C. 2012) (Comcast's disclosure of city and state information for subscribers that Plaintiff identified by IP address was not PII); *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 335-37 (E.D. Pa. 2012) (dismissed class action alleging disclosure of HIPPA-protected patient information for failure to state a claim; defendant sold "de-identified" prescription information to vendors who potentially could "re-identify" the information; no evidence that they had done so; proof would have been expert testimony about the risk of re-identification).

Plaintiffs argue that someone who possesses a unique identifier for an individual "requires no further information to distinguish the individual from the rest of the population." Opposition, ECF No. 155 at 9 (quoting Calandrino Decl. ¶ 28). But the issue is whether a unique identifier – without more – violates the VPPA. It does not. The VPPA prohibits the disclosure of a particular person's viewing choices to "any person," meaning, a third party. *See* 18 U.S.C. § 2710(b). The VPPA requires identifying the viewers and their video choices.

Plaintiffs also analogize to 16 C.F.R. § 312, the FTC's rule that defines personal information under the Children's Online Protection Act broadly to include persistent identifiers in cookies or online information that is combined with an identifier. Opposition, ECF No. 155 at 10. Protection of children online implicates different privacy concerns and resulted in broader definitions of personal information. By contrast, the VPPA prohibits only disclosure of a particular viewer's watched videos.

The next sections apply this analysis to the three disclosures, which differ in the information disclosed about a Hulu user and what happened with the disclosure.

1. Disclosure to comScore of Watch Page and Hulu User IDs

Hulu's liability here is based on the hypothetical that comScore could use the Hulu ID to access the Hulu user's profile page to obtain the user's name. Hulu characterizes this argument as "reverse engineering" its data. The idea is that comScore could capture the data from the watch page, extract the relevant information (the video name and Hulu User ID), and plug the data into the standard-format URL for the profile page to capture the user's name from that page. There is no evidence that comScore did this. The issue is only that it could.

At summary judgment, Hulu carried its initial burden by pointing to the absence of information that comScore correlated any information such that there is a disclosure within the meaning of the VPPA: "information which identifies a person as having requested or obtained specific video materials or services." *See* 18 U.S.C. § 2710(a)(3). Plaintiffs did not point to any evidence showing genuine disputes on any material fact about whether comScore did anything with the information. The evidence shows comScore's role in measuring whether users watched the advertisements. It also demonstrates comScore's interest in recognizing users and tracking their visits to other websites where comScore collects data. That information likely is relevant to an advertiser's desire to target ads to them. It does not suggest any linking of a specific, identified person and his video habits. The court grants summary judgment in Hulu's favor on this theory.[4]

2. The comScore UID (User ID) Cookie

For similar reasons, the court grants Hulu summary judgment on this theory. The disclosure is that Hulu coded the hulu.com watch pages to cause the user's web browser to send comScore a "comScore ID" that was unique to each registered user. These unique cookies allow comScore to recognize users and track their visits to other websites where comScore collects data. The point of the cookies is to recognize users to collect data about them, and here, that data included video choices. *See* Opposition, ECF No. 155 at 17-19; Calandrino Decl. ¶¶ 48-56, ECF No. 160-5; Wills Decl. ¶ 36, ECF No. 160-6 at 10. Looking at the evidence very practically, comScore doubtless collects as much evidence as it can about what webpages Hulu users visit. Its cookies help it do that. There may be substantial tracking that reveals a lot of information about a person. The cookies may show someone's consumption relevant to an advertiser's desire to target ads to them. And there is a VPPA violation only if that tracking necessarily reveals an identified person and his video watching. There is no genuine issue of material fact that the tracking here did that. The fact that Hulu wrote the code that sent the cookie does not alter this conclusion.

---

[4] comScore submitted a declaration in support of Hulu's opposition to Plaintiffs' class certification motion saying that it did not use any information it collected from hulu.com to personally identify any of Hulu's users or to link their PII to their requested or watched videos on hulu.com. *See* Johnson Decl., ECF No. 143, ¶ 12. The court does not rely on that declaration here.

3. Disclosure to Facebook of Watch Page and Transmission of Facebook Cookies to Facebook.

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. At the summary judgment stage, it is not clear to the court whether the datr cookie alone establishes a VPPA violation because it apparently reveals only the browser, and it is not clear that it is the linking of the specific, identified person to his watched videos that is necessary for a VPPA violation. *See* Calandrino Decl., ECF No. 160-5, ¶78.[5] But 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-iniated transmission of information.

Hulu argues that it never sent the "actual" name of any Facebook user. *See* Motion, ECF No. 125-4 at 22. Instead, the name came from the user's web browser and the interaction that Facebook had with its users. *Id.* It argues that this data transfer is based on standard Internet processes, without Hulu's involvement." *Id.* at 12. The "standard Internet process" is described above in the section of the Statement on cookies. *See supra* Statement, "III. How Hulu Interacts with comScore" (describing cookies). The user types a website address into the browser (e.g., www.facebook.com), and the browser sends a request to load the page along with the remote website's cookies that are already stored on the user's computer (here, the lu and c_user cookies). *See* Wu Decl., ECF No. 125-7, ¶ 15.

The Hulu-Facebook interaction here was a Hulu-prompted request from the Hulu user's browser

[5] According to a declaration filed in support of Plaintiffs' motion for class certification, the Facebook datr cookie value uniquely corresponds to a particular Facebook user, whether or not the user is logged into Facebook, and it can track the user's activity on Facebook and on other websites and associate it to the user's Facebook profile information. *See* Wills Decl., ECF No. 160-6, ¶ 42a. Despite that declaration, it apparently identifies only the browser.

to Facebook to load the Like button (as opposed to a user's request to load a Facebook page or a Hulu user's clicking on the Like button) that occurred before Facebook sent any data or instructions or cookies. *Id.* ¶ 59. According to Plaintiffs, Hulu wrote the code that sent the lu and c_user cookies stored on the Hulu user's computer that had information about the Hulu user's actual identity on Facebook. This is not merely the transmission of a unique, anonymous ID; it is information that identifies the Hulu user's actual identity on Facebook. The transmission was not the Hulu/Facebook user's decision. Instead, it was done automatically using Hulu's code to load the Facebook Like button. It may be true – as Hulu says – that accessing a remote browser involves sending that browser's cookies. But according to Plaintiffs' expert, it was straightforward to develop a webpage that would not communicate information to Facebook. *Id.* ¶ 57. 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.

Those Facebook ID cookies (the lu and c_user cookies) were transmitted with the watch page and the embedded video name. Thus, the process was an electronic transmission of the Hulu user's actual identity on Facebook and the video that the Facebook user was watching. *See* Calandrino Decl. ¶¶ 67-69 (the cookies transmitted the user's Facebook ID). Depending on Hulu's knowledge, that could be a VPPA violation. The 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.

Hulu argues that it needed to send an actual name to be liable and that it sent only cookies. Motion, ECF No. 125-4 at 22-23. The statute does not require an actual name and requires only something akin to it. If the cookies contained a Facebook ID, they could show the Hulu user's identity on Facebook. According to Plaintiffs' expert, "persons registered on Facebook must provide their real names when creating Facebook accounts." Wills Decl. ¶ 50. More to the point, a Facebook user – even one using a nickname – generally is an identified person on a social network platform. The 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.

Code is a language, and languages contain names, and the string is the Facebook user name. There is a material issue of fact that the information transmitted to Facebook was sufficient to identify individual consumers. *See* Calandrino Decl., ECF No. 160-5, ¶¶ 68-69, 79-81.

Hulu also argues 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. Reply Brief, ECF No. 140 at 8-9 (citing Calandrino Decl. ¶ 66). That may be so for devices with multiple users. It also is a fact issue. Again assuming Hulu's knowledge, there could be VPPA violations for users who were the only users of their devices or browsers. Also, Plaintiffs limit their statutory damages to one VPPA violation.

Hulu also argues that there is no evidence that Facebook took any actions with the cookies after receiving them. JSUF #25. It also says that there is no evidence that Facebook tied its Facebook user cookies to the URL for the watch page (and the accompanying title). Motion, ECF No. 125-4 at 15, 24. In contrast to comScore, where the user was not tied to the video in one transmission, the transmission to Facebook included the video name and Facebook user cookies. Thus, the link between user and video was more obvious. But Hulu's point is that the information really was not disclosed to Facebook in the sense that the information about Judge Bork's video viewing was disclosed to the Washington Post.

Whether this link was the equivalent of a disclosure under the VPPA depends on the facts. One can think of analogies in a paper world. Throwing Judge Bork's video watch list in the recycle bin is not a disclosure. Throwing it in the bin knowing that the Washington Post searches your bin every evening for intelligence about local luminaries might be. The issue is whether Hulu made a "knowing" disclosure.

The statute requires a "knowing" disclosure "to any person." *See* 18 U.S.C. § 2710(b)(1). The emphasis is on disclosure, not comprehension by the receiving person. *See* S. Rep. 100-599, at *12 ("[s]ection 2710(b)(1) establishes a statutory presumption that the disclosure of personally identifiable information is a violation" unless a statutory exception applies). Thus, the Seventh Circuit held that the practice of placing PII on parking tickets in the view of the public was a disclosure that violated the analogous Driver's Privacy Protection Act, regardless of whether anyone

viewed the PII. *See Senne v. Village of Palatine Ill.*, 695 F.3d 597 (7th Cir. 2012) (en banc). By analogy, if a video store knowingly hands a list of Judge Bork's rented videos to a Washington Post reporter, it arguably violates the VPPA even if the reporter does not look at the list.

Still, disclosure of information on traffic tickets in public view or providing a list of videos is different than transmission of cookies tied to a watch page. The first disclosures transmit obvious PII. The second transmits cookies with identifying information that is the equivalent of a name only to someone who has the ability to read it. Moreover, the VPPA prohibits a knowing disclosure to "any person," and the point of that prohibition is to prevent disclosure of a person's video viewing preferences to someone else.

No case has construed the word "knowingly" as it appears in the VPPA. Other 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. *See Freedman v. America Online, Inc.*, 329 F. Supp. 2d 745, 748-89 (E.D. Va. 2004) (faxing subscriber information to a police officer was knowingly divulging information protected by the Electronic Communication Privacy Act, 18 U.S.C. § 2701); *Muskovich v. Crowell*, No. 08 C 50015, 1996 WL 707008 (S.D. Iowa Aug. 30, 1996) (MCI employee obtained customer's private phone number from records; MCI's failure to implement adequate security procedures was not a knowing divulgement of her information).

Here, considering the statute's reach, the conclusion is that Hulu's transmission of the Facebook user cookies needs to be the equivalent of knowingly identifying a specific person as "having requested or obtained specific video materials or services." *See* 18 U.S.C. § 2710(a)(3). 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.

The issue then is what do the undisputed facts show about what Hulu knew. Hulu points to the parties' joint undisputed fact that "[n]o evidence has been introduced that Facebook took any actions with the [datr, lu, and c_user] cookies . . . after receiving them." JSUF #25. That the parties did not introduce evidence does not obviously end the inquiry. On the one hand, Facebook did receive the

packets of information (specific user information and videos watched) together. That is different than the comScore disclosures, which required comScore to tie information together in non-obvious ways. On the other hand, the Facebook user cookies are more like the Comcast hexidecimal customer codes that could identify a customer in *Pruitt*. The court's view is that if Hulu never knew that Facebook might "read" the videos and the Facebook ID cookies together in a manner akin to the disclosure of Judge Bork's videos, then there is not a VPPA violation. The problem here is that the JSUF shows only that there is no evidence "introduced" on whether Facebook took any actions with the Facebook ID cookies. That is not the same as saying, "there is no evidence at all." For example, it might be dispositive if Facebook could not auto-authenticate a user when the Like button loaded.

Hulu's next argument is that the cookies are "unintelligible" and "owned by Facebook[, and, a]s a result, Hulu cannot access that cookie or read information stored in it" and "could not have known what data Facebook was receiving. Accordingly, even if Facebook was collecting identifying information, Hulu did not 'knowingly' disclose that information to Facebook." Motion, ECF No. 125-4 at 17. Hulu's only evidentiary support for this argument is the following paragraph:

> The domain value for cookies means that the only servers which can access browser cookies are the servers associated with the domains that wrote the cookies. Therefore, a webserver associated with hulu.com will only access cookies with the domain hulu.com and a webserver associated with facebook.com will only access cookies with the domain facebook.com.

Wu Decl., ECF No. 125-7, ¶ 21.

This description – that only servers associated with the domain that writes a cookie can access that domain's cookie – does not answer the question about what Hulu knew. Instead, it only describes how servers can read cookies. 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. *See Celotex*, 477 U.S. at 325. Thus, the burden does not shift to Plaintiffs to submit admissible evidence showing a genuine issue for trial. That being said, there is additional information that

suggests fact issues about Hulu's knowledge.

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. *See supra*; Wu Decl., ECF No. 125-7, ¶ 25.

Emails about cookie placement establish that Hulu knew that vendors can place cookies on the user's computer. *See, e.g.*, Carpenter Decl. Ex. 11. Emails also show Hulu knew that cookies with identifying information were sent, Hulu's awareness that vendors could collect data and use it for other purposes to build a profile or "identify a user in the real world," and Hulu's recognition of the VPPA implications. *See* Carpenter Decl. Ex. 1; *id.* Ex. 5, HULU_GAR 177541 (noting VPPA implications); *id.* Ex. 9, HULU_GAR 19274 (concern with sending video titles to eHarmony). Another email states, "there are concerns around using beacons that send user data, along with the referrer ID, on a user-identifiable basis. Even with contractual restrictions, we can't rule out the possibility that someone might object to these practices for these or other reasons. But I said that Hulu had made the judgment that it would accept that legal risk given the business benefits of these analytics." *See id.*, Ex. 5, HULU_GAR 164822; *see id.* at HULU_GAR 164825 (Hulu made the judgment to accept the risk of passing identifying data "so long as it is not passing unique, identifying information, which sounds like you might be doing here . . . .").

These 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. And again, 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.

With comScore, again, the purposefulness of cookie use was less consequential given (a) the steps that comScore would need to take to tie the video to an identified user and (b) the reality of

comScore's business model. That is why there are no issues of material fact as to comScore. With Facebook, the cookies are transmitted when the watch page with the video name loads, and the point of the transmission is to load the Like button. The process of loading the Like button was not the decision of the Facebook/Hulu user, and instead, Hulu wrote the code that transmitted identifying information without that user's permission. If Hulu and Facebook negotiated the exchange of cookies so that Facebook could track information (including watched videos) about its users on Hulu's platform when the Like button loaded, or if Hulu knew that it was transmitting Facebook ID cookies and video watch pages, then there might be a VPPA violation. The record shows fact issues about Hulu's knowledge.

Another reason to deny summary judgment on this record is that this was an early summary judgment motion before the close of discovery. Plaintiffs are reviewing documents and source code still, and the motion was filed before this review and the class certification hearing. *See* Opposition, ECF No. 155 at 6. The court cannot dispose of a case involving fact questions about knowledge on an undeveloped record with a half-page argument about knowledge at the end of a brief that mostly is directed to Hulu's main argument that the alphanumeric strings here are not unique identifiers equivalent to a name.

The court denies Hulu's summary judgment motion regarding the disclosures to Facebook.

C. Whether Facebook Users Consented to the "Like" Button's Function

The VPPA permits disclosure to any consumer with the consumer's informed, written consent. During the class period, the VPPA's consent provisions – later amended effective January 2013 – required "the informed, written consent of the consumer given at the time the disclosure is sought." 18 U.S.C. § 2710(b)(2)(B). Hulu cites only Facebook's current policies and information on its Help Center in September 2013. Motion, ECF No. 125-4 at 24-25. There is no evidence about the policies in place during the class period of April 21, 2010 to June 7, 2012. If the 2013 Facebook policies were in place then (and it seems doubtful), Hulu did not say so. Also, Hulu does not explain why Facebook's data policies are the equivalent of the VPPA's "informed, written consent at the time of disclosure." Hulu's only legal argument is its citation to a case about how an online "click-to-accept-terms" form can result in a contract. *See id.* at 25. The court cannot conclude on this

record, with this argument, and as a matter of law that there was consent.

CONCLUSION

The court **GRANTS** Hulu's motion for summary judgment on the comScore disclosures and **DENIES** the motion for the disclosures to Facebook. This disposes of ECF No. 125-4.

IT IS SO ORDERED.

Dated: April 28, 2014

LAUREL BEELER
United States Magistrate Judge