UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALEXANDER YERSHOV, individually and on behalf of all others similarly situated,	
Plaintiff,	**Civil Action No. 14-13112-FDS**
v.	
GANNETT SATELLITE INFORMATION NETWORK, INC., dba USA TODAY,	
Defendant.	

MEMORANDUM AND ORDER ON
DEFENDANT'S MOTION TO DISMISS

SAYLOR, J.

This is a putative class action arising out of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710. The VPPA, among other things, prohibits the disclosure of "personally identifiable information" of certain consumers of video services. Plaintiff Alexander Yershov has filed suit against defendant Gannett Satellite Information Network, Inc.

Gannett publishes a print and on-line newspaper called *USA Today*. Gannett has also created a mobile app, called the "USA Today App," that is designed to run on smartphones and other mobile devices, and that permits readers to view the on-line version of the newspaper. Viewers using the App can access video clips on various news, sports, and entertainment topics. Plaintiff alleges that defendant discloses "personally identifiable information" every time a person uses the USA Today App to watch video clips. Specifically, plaintiff alleges that every time a user of the App watches a video, the unique identification number of the user's

smartphone is provided to a third-party data-analytics company. Plaintiff contends that by doing so, Gannett violates the VPPA.

On September 19, 2014, defendant filed a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(1) for lack of subject-matter jurisdiction and Fed. R. Civ. P. 12(b)(6) for failure to state a claim. For the following reasons, defendant's motion will be granted.

I. Background

A. The USA Today App

Gannett Satellite Information Network, Inc., is based in McLean, Virginia. (Compl. ¶ 6). Gannett is a media company that produces news and entertainment programming. (*Id.* ¶ 1). It distributes that content to consumers through a variety of media, including its flagship newspaper, *USA Today*. (*Id.*). In addition to the print edition of *USA Today*, Gannett offers content through websites and mobile software applications. (*Id.*). One of Gannett's mobile applications is the USA Today App. (*Id.* ¶ 2).

The USA Today App is a mobile software application that allows individuals to access news and entertainment media content. (*Id.* ¶ 9). It is available for installation on Android mobile devices, among others. (*Id.*). Android is a mobile device operating system developed by Google. (*Id.* ¶ 1 n.1). Smartphones made by a variety of companies, including HTC and Samsung, use the Android operating system. (*Id.*). Users can install the USA Today App on an Android device by visiting the Google Play Store, the on-line media platform operated by Google. (*Id.* ¶ 10). Once installed, the App allows users to view articles and video clips organized into sections, such as news and sports. (*Id.* ¶ 12). Prior to using it for the first time,

the App requests permission from users to "push" notifications on their device. (*Id.* ¶ 10).[1] The App does not otherwise seek a user's consent to disclose personal information to third parties for any purpose. (*Id.* ¶ 11).

There is no charge to install the App or to view video clips after installation. (*See* Compl. ¶¶ 9-11 (citing *USA Today*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.usatoday.android.news&hl=en (last visited July 2, 2014))). There is no registration requirement (such as a requirement that the user provide a name and e-mail contact). (*See id.*). After responding to the request for permission to "push" notifications, the user is not required to provide any other information in order to use the App. (*See id.*).

B. Alleged Transmittal of PII

The complaint alleges that each time users view video clips on the App, it sends a record of the transaction to Adobe Systems, Inc., an unrelated company that, among other things, performs third-party data-analytics. (*Id.* ¶ 13).[2] Along with the record of the transaction, the App sends a user's GPS coordinates and the Android device's unique identification number (the "Android ID"). (*Id.* ¶ 13). The Android ID is a "64-bit number (as a hex string) that is randomly generated when the user first sets up the device and should remain constant for the lifetime of the user's device." (*Id.* ¶ 13 n.3 (citing *Settings.Secure*, ANDROID DEVELOPERS, http://developer.android.com/reference/android/provider/Settings.Secure.html#Android_ID)). Android IDs are unique to specific devices and users. (*Id.* ¶ 16). It is not precisely clear what

[1] "Push" notifications are alerts that inform app users of relevant activity related to the app even when the user is not actively using it. USA Today App users may decline to receive "push" notifications. (*See id.* ¶ 10).

[2] The complaint characterizes Adobe as a data-analytics company that "provides insights into the behaviors and demographics for the App's user base." (*Id.* ¶ 19).

the "record of the transaction" includes, but it appears from the complaint that it includes an identification of the video watched by the user. (*See id.* ¶¶ 42, 54, 57).

According to the complaint, Adobe "collects an enormous amount of detailed information about a given consumer's online behavior (as well as unique identifiers associated with a user's devices) from a variety of sources." (*Id.* ¶ 20). "Once Adobe links a device's Android ID with its owner, it can then connect new information retrieved from Android apps—including the USA Today App—with existing data in the person's profile (which was previously collected by Adobe from other sources)." (*Id.* ¶ 22). Therefore, when Adobe receives an individual's Android ID and the record of the video transaction from USA Today App, it is able to connect that information with information collected from other sources "to personally identify users and associate their video viewing selections with a personalized profile in its databases." (*Id.* ¶ 29).

According to the complaint, Alexander Yershov downloaded and began using the USA Today App on his Android device in late 2013. (*Id.* ¶ 39). He never consented to allowing USA Today to disclose his "personally identifiable information" to third parties. (*Id.* ¶ 40).

The complaint alleges that "the combination of his device's unique Android ID and the records of videos that [Yershov] viewed . . . constitutes 'personally identifiable information' . . . because it allows Adobe to identify users such as Yershov, and to attribute their video-viewing records to their Adobe-created profiles." (*Id.* ¶ 57).

C. Procedural Background

Plaintiff filed the complaint in this action on July 24, 2014, alleging a violation of the Video Privacy Protection Act, 18 U.S.C. § 2710. (Compl.). The complaint is a putative class

action; the class is defined as "[a]ll persons in the United States who used the USA Today App to watch videos and had their PII transmitted to Adobe." (*Id.* ¶ 43). The complaint alleges that all such class members "have had their statutorily defined right to privacy violated." (*Id.* ¶ 62).

Defendant has moved to dismiss for failure to state a claim upon which relief can be granted.

II. Legal Standard

On a motion to dismiss, the Court "must assume the truth of all well-plead[ed] facts and give . . . plaintiff the benefit of all reasonable inferences therefrom." *Ruiz v. Bally Total Fitness Holding Corp.*, 496 F.3d 1, 5 (1st Cir. 2007) (citing *Rogan v. Menino*, 175 F.3d 75, 77 (1st Cir. 1999)). To survive a motion to dismiss, the complaint must state a claim that is plausible on its face. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). That is, "[f]actual allegations must be enough to raise a right to relief above the speculative level, . . . on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Id.* at 555 (citations omitted). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 556). Dismissal is appropriate if the facts as alleged do not "possess enough heft to show that plaintiff is entitled to relief." *Ruiz Rivera v. Pfizer Pharm., LLC*, 521 F.3d 76, 84 (1st Cir. 2008) (alterations omitted) (internal quotation marks omitted).

III. Analysis

The Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, was enacted in 1988. Congress passed the VPPA after a "newspaper in Washington published a profile of [Supreme

Court nominee and D.C. Circuit] Judge Robert H. Bork based on the titles of 146 films his family had rented from a video store." S. Rep. 100-599, 2d Sess. at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342.

Among other things, the VPPA prohibits "video tape service providers" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider" without the consumer's informed, written consent. 18 U.S.C. § 2710(b). The statute has three relevant definitions:

- the term "video tape service provider" means "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 term "personally identifiable information" "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); and
- the term "consumer" "means any renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1).

For present purposes, at least, defendant does not contest that it fits within the statutory definition of a "video tape service provider."[3] Defendant contends, however, that the complaint should be dismissed because (1) defendant did not disclose "personally identifiable information" within the meaning of the statute, (2) plaintiff is not a "consumer" within the meaning of the

[3] Although defendant contends that plaintiff's "VPPA claim will ultimately fail for the additional, independent, reason that Gannett is not a 'video tape service provider' under the VPPA," it does not challenge "the sufficiency of [p]laintiff's pleading" of this issue at this stage of litigation. (Defs.' Mem. Support Mot. Dismiss 7 n.4).

statute, and (3) plaintiff lacks standing because he has not pleaded an injury in fact.

A. Personally Identifiable Information

As noted, the VPPA prohibits "video tape service providers" from disclosing "personally identifiable information" ("PII") concerning a "consumer" to third parties. 18 U.S.C. § 2710(b). The complaint alleges that each time users view video clips on the USA Today App, defendant sends a record of the transaction along with the user's GPS coordinates and the Android ID for the user's device.[4] The first issue is whether that information sent to Adobe qualifies as "personally identifiable information."

Any statutory analysis begins with the text of the statute. To some extent, of course, this exercise involves an attempt to place a square peg (modern electronic technology) into a round hole (a statute written in 1988 aimed principally at videotape rental services). Nonetheless, the statute says what it says, and the place to begin is with the words themselves. Again, the VPPA provides that "personally identifiable information" 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). Those words must be interpreted in "context and with a view to [their] place in the overall statutory scheme." *Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989). Here, the statute provides at least two clues as to the meaning of the term.

First, the statute permits disclosure of PII under five specific circumstances. 18 U.S.C. §

[4] The complaint alleges that "even '[w]hen a device has multiple users [] each user appears as a completely separate device, so the ANDROID_ID value is unique to each user." (Compl. ¶ 17 (citing *Settings.Secure*, ANDROID DEVELOPERS, https://developer.android.com/reference/android/provider/Settings.Secure.html#ANDROID_ID (last visited July 15, 2014)). As a result, each device user has a unique Android ID. (*See id.*). It further alleges that Adobe is able to use the Android ID "to identify [plaintiff] and attribute his video viewing records to an individualized profile of [him] in its databases." (Id. ¶ 42).

2710(b)(2). One of those circumstances is that disclosure may be made "to any person" if "the disclosure is solely of the names and addresses of consumers," but only if the consumer has had an opportunity to prohibit that disclosure, and if the disclosure does not identify the "title, description, or subject matter of the video."[5] *Id.* § 2710(b)(2)(D). That suggests (1) that a consumer's name and address are both PII, and (2) that the universe of PII is greater than the consumer's name and address.

Second, the list of statutory definitions uses the word "means" in three out of four instances (in other words, the definitions are formatted to provide that the term "x" *means* "y"). *See* 18 U.S.C. § 2710(a)(1), (2), (4). As to PII, however, the statute provides that "the term 'personally identifiable information' *includes* information which identifies a person . . . ." *Id.* § 2710(a)(3) (emphasis in original). This suggests that the statutory term may have a broader definition than what is provided in the text, which may be a mere example of a possible form of PII.[6]

With that framework in mind, the Court turns to the question whether the information sent to Adobe constitutes PII. When a user requests a video clip, Gannett discloses three kinds of information: (1) a record of the transaction (presumably, information concerning the precise video selected for viewing); (2) the user's GPS coordinates (that is, the precise location of the user); and (3) the Android ID of the user's smartphone or other device. There is no question that

[5] The statute provides an exception, such that "the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer." 28 U.S.C. § 2710(b)(2)(D)(ii).

[6] While the Court places very limited weight on legislative history, that history supports such a conclusion. According to the Senate Report, Congress's purpose in enacting the VPPA 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, 2d Sess. at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342. at *1. The Senate Report specifically notes that the definition of PII "uses the word 'includes' to establish a minimum, but not exclusive, definition . . . ." *Id.* at *11.

the information transmitted to Adobe identifies the "specific video materials or services" requested or obtained by the consumer. *See* 18 U.S.C. § 2710(a)(1)(3). The issue is whether that information also identifies a specific person.

Without question, a person's name, social security number, and date of birth are PII. *See In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003) (finding that the definition of "contents" in Electronic Communication Privacy Act encompasses "personally identifiable information such as a party's name, date of birth, and medical condition").[7] Similarly, a person's home address is PII, under the statutory construction noted above and as a matter of common sense.[8] Similar types of information, such as a place of birth, a mother's maiden name, an automobile license plate number, or a home telephone number, could also be PII under at least some circumstances; for example, celebrities and public officials often have unlisted telephone numbers and "blocked" license plate numbers in order to protect their privacy and security.

It requires no great leap of logic to conclude that the unique identifier of a person's smartphone or similar device—its "address," so to speak—is also PII. A person's smartphone

---

[7] Several federal statutes contain provisions that specifically use the term "personally identifiable information" or similar terms. *See, e.g.*, 20 U.S.C. § 1232g (Family Educational Rights and Privacy Act); 47 U.S.C. § 551(a)(2) (Cable Communications Policy Act); *see also* 15 U.S.C. § 6809(4)(A) (The Gramm-Leach Billey Financial Modernization Act) (referring to "nonpublic personal information").

[8] The Family Education and Records Privacy Act of 1974 ("FERPA") prohibits educational entities from releasing or providing access to "any personally identifiable information in education records." 20 U.S.C. § 1232g(b)(2). The statute does not provide a definition for PII. However, the regulation implementing the statute provides the following definition:

> The term includes, but is not limited to—(a) The student's name; (b) The name of the student's parent or other family members; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty . . . .

34 C.F.R. § 99.3.

"address" is an identifying piece of information, just like a residential address. Indeed, it is in many ways a more significant identifier. Smartphones typically contain "vast quantities of personal information." *Riley v. California*, 134 S. Ct. 2473, 2485 (2014). "[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Id.* Therefore, the type of information that could be ascertained from a smartphone could potentially be devastating to an individual's privacy interests. A person with access to a smartphone's unique identifer could potentially learn a huge quantity of personal information about the user of that smartphone. Furthermore, a smartphone may be more directly connected to a specific individual that even a residential address; for example, people are much more likely to share their homes with other persons than their smartphones.

Defendant makes two principal objections to that conclusion. First, it contends that the Android ID cannot be PII because it identifies an object, rather than a human being. But that contention cannot be correct. A home address describes an object, not a person, but there can be little doubt that it is PII. Indeed, and as noted, the VPPA expressly refers to the "addresses of consumers," in a context clearly indicating that an address is PII. And that is true even though multiple persons may share a residence.[9] The identity of an object—its unique "address," whether in the physical world or in cyberspace—can therefore constitute PII, at least under some circumstances.

Next, defendant contends that the Android ID cannot be PII because that information

[9] Similarly, an automobile license plate number or a home telephone number may identify an object (a motor vehicle or a telephone) that several persons (for example, spouses or teenage children of the owner) may share. Nonetheless, that type of information could be a personal identifier under many circumstances, and thus fit within the definition of the statute.

cannot be linked to a specific person without access to certain additional information—specifically, the information that a particular phone is used by a particular person. But that is true of every identifier other than a person's name. For example, a social security number is a string of nine numbers that only takes on meaning if it can be identified as the number of a specific person. Likewise, a date in a calendar is meaningless as an identifier, unless it is identified as a specific person's date of birth. Even a person's name may be of limited use as an identifier without further information; there may be hundreds, or thousands, of persons with the same or a similar name.

At oral argument, defendant conceded that a home address qualifies as PII even though it requires an extra step to link it to a specific person. Defendant contended, however, that home addresses qualify as PII because there are public record databases that can link home addresses to individuals, but there is no such publicly accessible database that links an Android ID to a person. Defendant therefore contended that in isolation the Android ID is a meaningless number. But the same could also be said for social security numbers. There is no publicly accessible database that links those numbers to individuals, but a social security number is nonetheless unquestionably the type of information that fits within the definition of PII.

It is also noteworthy that Gannett transmits the GPS coordinates of the user along with the Android ID. Presumably, that information would be sufficient to identify a very specific location (such as a building) from which the user viewed the video. It therefore appears possible to identify, with a relatively high degree of accuracy, the residential address of users at the same time as their Android ID. Indeed, in areas of relatively low-density housing, the GPS coordinates of the user are essentially identical to a residential address.

Finally, defendant notes that the substantial weight of authority points in the opposite direction. Of particular relevance is the Northern District of Georgia's ruling in *Ellis v. Cartoon Network, Inc.*, 2014 WL 5023535 (N.D. Ga. Oct. 8, 2014), because its facts are very similar to the facts of the present case.

In *Ellis*, the court examined whether the Cartoon Network App's transmission of a user's video history along with the user's Android ID to a third party constituted a violation of the VPPA. *Id.* at *2. For purposes of the motion to dismiss, the court accepted that the third party was able to reverse engineer the consumer's identities from the Android ID, using information previously collected from other sources. *Id.* at *1. In its analysis, the court found that PII "is that which, in its own right, without more, 'link[s] an actual person to actual video materials.'" *Id.* at *3 (quoting *In re Nickelodeon*, 2014 WL 3012873, *10 (D.N.J. July 2, 2014)). The court determined that the Android ID does not identify a specific person without the third party taking extra steps. *Id.* As a result, it concluded that "the disclosure of an Android ID alone . . . does not qualify as personally identifiable information under the VPPA." *Id.* It relied on district court decisions in *In re Hulu Privacy Litigation*, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014), and *In re Nickelodeon Consumer Privacy Litigation*, 2014 WL 3012873 (D.N.J. July 2, 2014), to come to its conclusion.[10]

[10] Two other decisions that defendant cites in support of its motion to dismiss also rely on the *Hulu* and the *Nickelodeon* decisions to conclude that information similar to the Android ID is not PII. *See Locklear v. Dow Jones & Company, Inc.*, 1:14-cv-00744-MHC (N.D. Ga. Jan 23, 2015) (relying on the *Hulu*, *Nickelodeon*, and *Ellis* decisions to conclude that disclosure of Roku serial number and titles of videos does not violate the VPPA because the Roku serial number without more is not PII); *Eichenberger v. ESPN, Inc.*, C14-463 TSZ (W.D. Wash. Nov. 24, 2014) (relying on the *Hulu* decision to conclude that disclosure of Roku serial number and viewing records does not violate the VPPA because the Roku serial number is not PII). After the court in *Eichenberger* dismissed the first amended complaint, the plaintiff in that case filed a second amended complaint. *See Eichenberger v. ESPN, Inc.*, C-14-463 TSZ (W.D. Wash. May 7, 2015). The second amended complaint alleged that the third party, Adobe, was able to "automatically correlate[] [the Roku device serial number] with existing user information possessed by Adobe, and therefore identif[y] Eichenberger as having watched specific video material . . . ." *Id.* at 3. In an

The *Nickelodeon* case involved a class of children under the age of thirteen who sued Viacom for violating the VPPA. The case involved plaintiffs who visited "certain Viacom-owned websites and willingly provide[d] Viacom with their gender and age when they register[ed] as users of the sites." *Id.* at *2. When the plaintiffs went to these websites, Viacom also placed a "cookie" on their computer without their consent or that of their parents." *Id.* The "cookie" allowed Viacom to acquire certain information about each plaintiff, including their "'IP address'; 'browser settings'; 'unique device identifier'; 'operating system'; 'screen resolution'; 'browser version'; and certain 'web communications,' specifically 'detailed URL . . . requests and video materials requested and obtained from Viacom children's websites." *Id.* at *1. Whenever registered users watched video on Viacom's websites, Viacom made a record of that activity and shared it with Google. *Id.* at *1-2. The court refused to credit allegations in the complaint that Viacom and Google were able to link online activity and information with offline activity and information, and thereby "identify specific users." *Id.* at *2 n.3. Against that backdrop, the court examined whether Viacom's disclosures to Google of "anonymous usernames; IP address; browser setting; 'unique device identifier'; operating system; screen resolution; browser version; and 'detailed URL requests and video materials requested and obtained' from the Viacom websites, requests which presumably contain" gender and age information and the title of a video, violated the VPPA. 2014 WL 3012873, at *10. The court cited the *Hulu* decision as holding that "PII is information that must link 'a specific, identified

---

opinion issued on May 7, 2015, the *Eichenberger* court engaged in a more thorough analysis of PII by looking to the statutory text, "its legislative history, and the growing line of cases that have considered this issue." *Id.* at 6-12. The court cited the *Nickelodeon*, *Hulu*, *Ellis*, and *Locklear* decisions, and concluded that plaintiff's complaint did not sufficiently plead that the defendant had disclosed PII. *Id.* at 10. The court found that the allegation that Adobe could combine the Roku device serial number with other information already in its possession "also fails to assert a plausible claim to relief under the VPPA." *Id.*

person and his video habits'—what the *Hulu* [c]ourt characterizes as any information 'akin' to a name." *Id.* at *10 (quoting *Hulu*, 2014 WL 1724344, at *12, 14). The *Nickelodeon* court concluded that "PII is information which must, without more itself link an actual person to actual video materials." *Id.* The court found that "all Google knows from the disclosure of this information . . . is 'a child's username, sex, age, type of computer,' and IP address." *Id.* at *11. It is not enough that "information might one day serve as the basis of personal identification after some effort on the part of the recipient" because "the same could be said for nearly any type of personal information; this [c]ourt read the VPPA to require a more tangible, immediate link." *Id.* Because this information in isolation did not identify a person, the court concluded that plaintiff's VPPA claim against Viacom failed. *Id.* at *9.[11]

In *Hulu*, on a motion for summary judgment, the Northern District of California examined whether three types of disclosures by Hulu were PII. 2014 WL 1724344, at * 9. The first disclosure, to comScore, was a "watch page" URL web address that contained the video name and the Hulu user's unique seven-digit Hulu User ID. *Id.* Using the user ID, comScore could access a user's profile page, which listed the user's first and last name. *Id.* The second disclosure, to comScore, was a "comScore ID" that was unique to each registered user, which "allowed comScore to link the identified user and the user's video choices with information that

[11] In response to the court's decision, plaintiffs amended their complaint to "allege that Google could learn [p]laintiffs' actual identities by using a 'DoubleClick cookie identifier,' and by combining the information Viacom provides it with data it already gathers from its other websites and services." *In re Nickelodeon Consumer Privacy Litigation*, 2015 WL 248334, *2 (D.N.J. Jan. 20, 2015). In its unpublished opinion in the *Nickelodeon* case, the court found that plaintiffs did not allege "new facts which make it plausible that the information collected does indeed identify [p]laintiffs." *Id.* at *3-*4. The court confirmed its previous holding that PII "is information which must, without more, itself link an actual person to actual video materials." *Id.* at *3. Because the complaint alleged that Google independently gathered information to connect an actual person with actual video materials, the court concluded that the information disclosed by Viacom did not constitute PII. *Id.* In any event, the court found that the complaint included "no allegation that Google can identify the individual [p]laintiffs in this case, as opposed to identifying people generally, nor any allegation that Google has actually done so here." *Id.* at *4. As a result, the court dismissed the amended complaint. *Id.*

comScore gathered from other websites that the same user visited." *Id.* The third disclosure, to Facebook, included unique identifiers that sometimes consisted of the user's IP address, the URL web address with the video name, and the user's Facebook ID. *Id.* The court in *Hulu* found that "the statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person." *Id.* at *11. It therefore explained that "a unique anonymized ID could be PII if other evidence renders it the equivalent of identifying a specific person." *Id.* However, it also noted that case law supported a "conclusion that anonymous identification data alone is not PII.**"*** *Id.* In examining the three types of disclosures, the court looked at how the third party used the information. *Id.* at *12. The court concluded that the disclosure of the watch page URL containing the video name and a user's unique seven-digit Hulu User ID was not PII because there was no evidence that suggested any linking of a specific, identified person and his video habits. *Id.*. Likewise, the court concluded that the disclosure to comScore of the comScore ID was not PII on the ground that although "[t]here may be substantial tracking that reveals a lot of information about a person . . . [,] there is a VPPA violation only if that tracking necessarily reveals an identified person and his video watching." *Id.* Finally, the court concluded that the disclosure to Facebook of the watch page, the user's IP address, and the Facebook user ID was PII because it constituted information that identified the Hulu user's actual identity on Facebook. *Id.* at *13. "If the cookies contained a Facebook ID, they could show the Hulu user's identity on Facebook." *Id.* at *14.

The *Hulu* decision does not necessarily support a finding that an Android ID is not PII.

The case was decided on a motion for summary judgment, and specifically noted 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." It is unclear whether the court meant that context could render it PII if other information provided in the disclosure with the anonymized ID identified a specific person, or whether context could render it PII if the third party receiving the information had independent information that helped link the ID with a specific person. No matter what it holds, it is clear that the inquiry is context-dependent. Based on the logic of the *Hulu* decision, it would appear that the factual record would need to be developed before concluding that an Android ID is not PII.

In any event, *Nickelodeon's* conclusion that "PII is information which must, without more, itself link an actual person to actual video materials" is flawed. That conclusion would seemingly preclude a finding that a home address or social security number is PII. Surely, that cannot be correct. Therefore, because it relies on *Nickelodeon* and *Hulu*, the holding in *Ellis* that an Android ID is not PII is unpersuasive.[12]

---

[12] Defendant also cites a variety of cases outside of the VPPA that involve PII to support its motion. For example, defendant cites the Cable Communication Privacy Act cases *Pruitt v. Comcast Cable Holdings, LLC*, 100 Fed. Appx. 713 (10th Cir. 2004) and *Klimas v. Comcast Cable Comm'ns., Inc.*, 2003 WL 23472182 (E.D. Mich. July 1, 2003), *aff'd on other grounds*, 465 F.3d 271 (6th Cir. 2006). Courts have found that the VPPA is analogous to the Cable Act. *See Parker v. Time Warner Entmt' Co.*, 1999 WL 1132463, at *9 (E.D.N.Y. Nov. 8, 1999).

In *Pruitt*, the Tenth Circuit examined whether Comcast information stored within Comcast's converter boxes is PII. 100 Fed. Appx. at 716. The court explained that "[i]ndividual subscriber information is not contained within the converter box, but an identifying number known as a 'unit address' allows Comcast to match the subscriber's purchases to its billing system." *Id.* at 715. The court determined that "the converter box code—without more—provides nothing but a series of numbers." *Id.* at 716. Because "without the billing information, even Comcast would be unable to identify which individual household was associated with the raw data in the converter box," the court concluded that information contained in the boxes is not PII. *Id.* at 716-17. The *Hulu* court found that "*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*, 2014 WL 1724344, at *11. Here, the complaint alleges that Adobe is able to use the Android ID to identify specific individuals.

In *Klimas*, 2003 WL 23472182, the plaintiff brought a class action alleging that Comcast "secretly

The opinions cited above seem to take an unrealistic view of the nature of personal identifiers, and how readily different databases or pieces of information can be linked together. The courts appear to frame the issue in large part by referring to these identifiers as "anonymous identifiers," which is unhelpful and possibly misleading. Again, a social security number or a date of birth, in isolation, is anonymous. However, it would be absurd to conclude that a social security number is not PII, simply because there is no publicly-available database linking those numbers with names.

Likewise, it is unrealistic to refer to PII as "information which must, without more, itself link an actual person to actual video materials." Again, that would appear to preclude a finding that home addresses, social security numbers, and dates of birth are PII. Moreover, drawing a link between the Android ID and a person's name may not be difficult. If, as alleged, Adobe collects information from the USA Today App linking an Android ID and GPS information with a specific video, and collects information from another source (such as GPS information linked to residential addresses, and residential addresses linked to names)—it would be relatively easy for Adobe to link that information to identify a person. It is also possible, of course, that third parties such as Adobe have access to databases that link Android IDs to specific persons.

In short, the information alleged disclosed to Adobe by Gannett, which consists of an Android ID and a GPS location, constitutes "personally identifiable information" within the meaning of the Video Privacy Protection Act.

---

intercept[ed], cop[ied], stor[ed], and otherwise collect[ed] all the information sent to and from its subscribers over the Internet" in violation of the Cable Act. Comcast admitted storing IP and URL information. The issue the court considered was whether dynamic IP addresses constitute PII. *Id.* at *4. The court found that "a dynamic IP address cannot constitute PII [because] [u]nlike a subscriber's name, address, social security number, etc., a dynamic IP address is constantly changing." *Id.* at *5. It is undisputed that the Android ID is static.

B. Plaintiff Is Not a "Subscriber"

The VPPA defines a "consumer" as any "renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710.(a)(1). Plaintiff contends that he is a "subscriber" for purposes of the VPPA because he "downloaded, installed, and watched videos" using the App.

The term "subscriber" is not defined in the statute. Traditionally—and certainly as of 1988, when the statute was enacted—a "subscriber" would have been defined principally as a person who has signed up to receive a periodical or a commercial service, typically having agreed to make a regular payment. *See, e.g.*, WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 1176 (Frederick C. Mish, et al., eds., 1991) (defining "subscribe" as "to enter one's name for a publication or service; also: to receive a periodical or service regularly on order"); *Subscriber Definition*, THE OXFORD ENGLISH DICTIONARY (online ed.), http://oed.com/view/Entry/192954?redirectedFrom=Subscriber#eid (last visited Apr. 2, 2015) (defining "subscriber" as "a person who makes a regular payment in return for entitlement to receive a periodical, membership of a society, access to a commercially provided service, etc.").[13] The traditional subscription business model involves an individual making periodic payments in exchange for delivery of magazines, newspapers, or other content. *See, e.g.*, *Subscribe to Home Delivery*, BOSTON GLOBE, http://services.bostonglobe.com/subscribers/homedelivery.aspx?id=5278 (last visited Apr. 14, 2015).

In the modern electronic world, subscriptions entail a broader spectrum of activity.

[13] Other definitions of "subscriber," such a person who signs one's name to a document, pledges a gift or contribution in writing, or agrees to purchase an offering of securities, are clearly not relevant here. *See Subscribe Definition*, MERRIAM-WEBSTER (online ed.), www.merriam-webster.com/dictionary/subscriber (last visited May 5, 2015).

Certain periodicals allow access (or complete access) to online content only with a subscription. *See, e.g.*, WASHINGTON POST https://subscribe.washingtonpost.com/acquisition/acquisitionapp.html#/offers/promo/digital01 (last visited Apr. 14, 2015); N.Y. TIMES, http://www.nytimes.com/subscriptions/Multiproduct/lp88U46.html?campaignId=4FWFJ&__KEYWORDS__=${keywordText}&__CAMP__=4FWFJ (last visited Apr. 14, 2015). In addition, individuals may subscribe to YouTube channels and podcasts. *Subscribe to the Channels You Love*, YOUTUBE, https://support.google.com/youtube/answer/4489286?hl=en (last visited Apr. 15, 2015); *Discovering Podcasts*, APPLE, https://www.apple.com/itunes/podcasts/discover/ (last visited Apr. 15, 2015).[14] A "subscriber" has also been defined as "a person who adds his or her details to an electronic newsgroup mailing list, etc., in order to receive, or contribute to, its contents; a person who has signed up to receive messages or other information from a newsgroup, mailing list, etc." *Subscriber Definition*, THE OXFORD ENGLISH DICTIONARY (online ed.), http://oed.com/view/Entry/192954?redirectedFrom=Subscriber#eid (last visited Apr. 2, 2015).

A common thread can be distilled from these definitions and examples. Subscriptions involve some or all of the following: payment, registration, commitment, delivery, and/or access to restricted content. To download and use the USA Today App, an individual does not have to pay any money; does not have to register; and does not have to make any commitment of any

[14] With a YouTube subscription, a person must register and then login to his or her account. *Subscribe to the Channels You Love*, https://support.google.com/youtube/answer/4489286?hl=en (last visited Apr. 15, 2015). The individual then clicks the "Subscribe" button for a specific channel. *Id.* Once an individual has subscribed to a YouTube channel, "the channel is added to [her] guide . . . . [W]henever [she] visits [her] homepage, new videos from [her] subscriptions will appear in the My Subscriptions feed." *Id.* This means that an individual receives "updates whenever [a channel] upload[s] new videos." *Id.* A podcast subscription is similar to a Youtube subscription. When an individual subscribes to a podcast, he or she will "automatically receive any future episodes." Podcasts are automatically delivered to individuals as they are uploaded. *Discovering Podcasts*, APPLE, https://www.apple.com/itunes/podcasts/discover/ (last visited Apr. 15, 2015).

kind. The complaint does not allege that downloading the App causes individuals to be placed on an e-mail list or permits individuals to access otherwise restricted content. To watch videos on the USA Today App, users simply click on the app and click on the video. The App appears to merely be a more convenient form of visiting the USA Today website.[15] Under the circumstances, an individual who downloads and uses the USA Today is not a "subscriber" within the meaning of the VPPA. In common parlance, an individual who watches video on the App is simply known as a "user."

That conclusion is bolstered by the fact that subscriptions do exist for other forms of apps. *See, e.g., Subscriptions on Google Play*, GOOGLE, https://support.google.com/googleplay/answer/2476088?hl=en (last visited Apr. 15, 2015); *Monetize Apps: Paid Apps vs. In-App Purchases vs. Freemium vs. Subscription*, BUILDBLOG BY THINKAPPS, http://thinkapps.com/blog/post-launch/monetize-apps-paid-apps-vs-app-purchases-vs-freemium-vs-subscription/ (last visited Apr. 15, 2015). According to Google, a "subscription is when you pay a recurring fee rather than a one-time price for content on Google Play. You'll automatically be charged at the beginning of each subscription term." *Subscriptions on Google Play*, *supra*. In its Buildblog, ThinkApps (which is an on-demand service for designing and building applications for web, mobile and wearables) explains that there are many different models for apps. *Monetize Apps*, *supra*. Among those models are paid apps, free apps, and subscription apps. *Id.* According to this blogpost, "[s]ubscription apps offer users access to a particular service or content for a weekly, monthly, or annual fee." *Id.* Thus, because there is a recognized concept of a subscription within the app context—and because users of the USA Today App do not fit within

[15] At oral argument, plaintiff appeared to concede that visiting the USA Today website alone would not make an individual a "subscriber" under the VPPA. (Mot. Hearing Tr. 29-30).

that concept—individuals who use the USA Today App are not "subscribers" within the VPPA's definition of "consumer."

Again, however, the weight of authority seems to point in the opposite direction. In *Ellis v. Cartoon Network*, the court relied on a 2012 decision in the *Hulu* case to conclude that an app user qualifies as a "subscriber." 2014 WL 5023535, at *2.[16] The *Ellis* court did not look to the plain meaning of "subscriber," and appeared to rely on the *Hulu* court's analysis as conclusive. *Id.* In *Hulu*, the defendant contended that plaintiff could not be a "subscriber" on the ground that the ordinary meaning of the term implied the payment of money. 2012 WL 3282960, at *7-8. The court determined that the plaintiffs in the *Hulu* case pleaded "more than just visiting Hulu's website." *Id.* at *8. The court concluded that because the term "subscriber" does not necessarily imply the payment of money, the plaintiffs in that case could be considered "subscribers."[17]

Again, this Court concludes that *Hulu*, and the cases that follow its reasoning, are not correctly decided. Here, at least, where there is no payment of money, no registration of information, no periodic delivery, and no privilege to view restricted content, none of the necessary elements of a subscription are present. Plaintiff is therefore not a "subscriber" within the meaning of the VPPA. Accordingly, the complaint fails to state a claim upon which relief can be granted.[18]

---

[16] The court in *Locklear v. Dow Jones & Co.*, 14-cv-00744-MHC (N.D. Ga. Jan. 23, 2015), relied on both *Ellis* and *Hulu* to conclude that an individual who downloaded the WSJ Channel and used it to watch video clips qualified as a "subscriber."

[17] It appears that *Hulu* involved registered users who received Hulu IDs, established Hulu profiles, and used Hulu's video streaming services. 2012 WL 3282960 at *7.

[18] The Court does not reach the question of whether the complaint alleges an injury in fact.

IV. Conclusion

For the foregoing reasons, the motion to dismiss is GRANTED.

So Ordered.

/s/ F. Dennis Saylor
F. Dennis Saylor IV
Dated: May 15, 2015 United States District Judge