ALSTON&BIRD

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

JUNE 17, 2015

District Court Rules a Unique Device Identifier Is Personally Identifiable Information for Purposes of the Video Privacy Protection Act

By Kim Chemerinsky and Dominique R. Shelton

The District of Massachusetts's decision in *Yershov v. Gannett Satellite Information Network, Inc.*, 1:14-cv-13112-FDS (D. Mass. May 15, 2015), adds additional fuel to the debate among the courts as to whether a unique device identifier may constitute personally identifiable information (PII) and whether a "subscription" requires payment under the Video Privacy Protection Act (VPPA).

Plaintiff Alexander Yershov filed suit against defendant Gannett Satellite Information Network, Inc., alleging violations of the VPPA. Gannett publishes *USA Today* and has created the USA Today app, a mobile app designed to run on smartphones and other mobile devices and permit readers to view the online version of the newspaper. Users of the app can access video clips on various news, sports and entertainment topics. In his lawsuit, the plaintiff alleged that Gannett violated the VPPA by disclosing PII in the form of unique device identifiers to third parties such as Adobe Systems, Inc., an analytics company.

On September 19, 2014, Gannett filed a motion to dismiss pursuant to Rules 12(b)(1) and 12(b)(6), arguing that, among other things, it did not disclose PII within the meaning of the VPPA. The court granted Gannett's motion, but departed from many courts in holding that a mobile device ID constitutes PII for purposes of the VPPA. The district court again departed from the weight of authority from other courts that have held that any user of a mobile application constitutes a "subscriber." Instead, the court held that to be a subscriber under the VPPA, the user must make some sort of periodic payment for the service provided.

Whether Gannett Disclosed Personally Identifiable Information Within the Meaning of the VPPA

The court rejected Gannett's assertion that the information Gannett allegedly disclosed—including a user's mobile device ID—was not PII within the meaning of the VPPA.

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

In the *Gannett* case, the plaintiff's complaint alleges that each time users view video clips on the app, the app sends a "record of the transaction" to Adobe. While it is not entirely clear what is meant by a "record of the transaction," it appears that the USA Today app at least conveys information sufficient to identify the videos watched by users. The complaint further alleges that 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.… 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)." Thus, when Adobe receives an individual's Android ID and the record of the video transaction from the USA Today app, it is able to connect that information with information from other sources "to personally identify users and associate their video viewing selections with a personalized profile in its databases." Specifically, when a user requests a video clip, Gannett discloses three kinds of information: (1) a record of the transaction (information related to the video selected for viewing); (2) the user's GPS coordinates (i.e., the precise location of the user); and (3) the Android ID of the user's smartphone or other device.

The court began its analysis noting that "[t]here is no question that the information transmitted to Adobe identifies the 'specific video materials or services' requested or obtained by the consumer." Thus, the court turned to the trickier question of whether the information sent to Adobe qualifies as PII. In doing so, the court noted that a person's name, social security number, date of birth and home address are PII, and that other types of information, such as a person's place of birth, mother's maiden name, automobile license plate number or home telephone number, may be PII under certain circumstances. The court reasoned:

> 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 "address" is an identifying piece of information, just like a residential address. Indeed, it is in many ways a more significant identifier.

Quoting the U.S. Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473, 2485 (2014), the court remarked that smartphones typically contain "vast quantities of personal information. … [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." For this reason, the Massachusetts district court noted, the type of information that can be ascertained from a smartphone may be "devastating" to a person's privacy interest: a person with access to a smartphone's unique ID "could potentially learn a huge quantity of personal information about the user of that smartphone."

The court's conclusion that the unique identifier of a person's smartphone or mobile device constitutes PII under the VPPA is diametrically opposed to the conclusions reached by other courts analyzing the same issue. For instance, in *Ellis v. Cartoon Network, Inc.*, 2014 WL 5023535 (N.D. Ga. Oct. 8, 2014), the United States District Court for the Northern District of Georgia granted the defendant's motion to dismiss, holding 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 Consumer Privacy Litig.*, MDL 2443 SRC, 2014 WL 3012873, at *10 (D.N.J. July 2, 2014)). Noting that the Android ID did not identify a specific person without a third party taking extra steps, the court determined that "the disclosure of an Android ID alone… does not qualify as personally identifiable information under the VPPA." Id. Likewise, in *Nickelodeon*, the United States District Court for the District of New Jersey dismissed a claim that Viacom violated the VPPA by disclosing to Google information such as a user's anonymous username, IP address and unique device identifier each time a user watched a video on Nickelodeon's websites. 2014 WL 3012873, at *10. In doing so, the court found that "there is simply nothing on the face of the statute or in its legislative history to indicate that 'personally identifiable information' includes the types of information… allegedly collected and disclosed by Viacom." *Id*.

Whether the Plaintiff Was a "Subscriber" Within the Meaning of the VPPA

Gannett also argued, and the court agreed, that Yershov was not a "consumer" within the meaning of the VPPA. The VPPA defines "consumer" as any "renter, purchaser, or subscriber of goods or services.…" Yershov argued that he was a "subscriber" because he "downloaded, installed, and watched videos" on the USA Today app.

The VPPA does not define "subscriber," but the court, having distilled definitions from several sources, concluded that "[s]ubscriptions involve some or all of the following: payment, registration, commitment, delivery, and/or access to restricted content." The court reasoned that the plaintiff was not a subscriber because he watched the video at no charge and did not make any payment at any time for the services provided by the app. Specifically, the court remarked: "[h]ere, 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." Accordingly, as the plaintiff was not a subscriber under the VPPA, the district court granted Gannett's motion to dismiss.

In concluding that to be a subscriber requires a user to make some periodic payment for the service provided, the court again departed from the majority of courts that have held that any user of a mobile application constitutes a subscriber under the VPPA. *See, e.g., In re Hulu Privacy Litig*., 2012 WL 3282960, at *7-8 (N.D. Cal. Apr. 28, 2014); *Ellis*, 2014 WL 5023535, at *2.

Our takeaway from this case is that the debate as to what constitutes PII and who is considered a consumer under the VPPA continues to rage on and the VPPA continues to serve as a potential vehicle for plaintiffs' lawyers to seek what they have described as "annihilating damages" from companies that stream video on their websites and mobile applications. Although the *Gannett* court granted the plaintiff's motion to dismiss, it should be noted that this was a near-miss: the court's decision as to both of the points described above departed from the overwhelming weight of authority analyzing these issues. Companies should be aware of the current heightened litigation and regulatory enforcement environment around privacy and take care to prioritize compliance in their video practices.

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

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

Members of Alston & Bird's Privacy & Security Group

Atlanta

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

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

David Carpenter
david.carpenter@alston.com
404.881.7881

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

Julia Dempewolf
julia.dempewolf@alston.com
404.881.7169

Maki DePalo
maki.depalo@alston.com
404.881.4280

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

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

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

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

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

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

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

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

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Peter Swire
peter.swire@alston.com
404.881.4259

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

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

Los Angeles

David Caplan
david.caplan@alston.com
213.576.2610

Kimberly K. Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

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

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

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

Evan Sippel-Feldman
evan.sippel-feldman@alston.com
213.576.1098

Washington, D.C.

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

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

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

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

Jason R. Wool
jason.wool@alston.com
202.239.3809

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON&BIRD

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333