No. 16-13031

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

RYAN PERRY,
Plaintiff-Appellant,

v.

CABLE NEWS NETWORK, INC., and
CNN INTERACTIVE GROUP, INC.,
Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of Georgia, Atlanta Division,
Docket No. 14 -02926
Hon. Eleanor L. Ross, District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF APPELLANTS

MARC ROTENBERG
ALAN BUTLER
AIMEE THOMSON
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., N.W., Suite 200
Washington, D.C. 20009
Tel: (202) 483-1140
Fax: (202) 483-1248

Counsel for Amicus Curiae

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Local Rule 26.1-1, *Amicus Curiae* Electronic Privacy Information Center ("EPIC") certifies that the following parties have an interest in the outcome of this appeal:

1. Andrews, Ryan D. (attorney for Plaintiff-Appellant)
2. Bakowski, Alan W. (attorney for Defendants-Appellees)
3. Balabanian, Rafey S. (attorney for Plaintiff-Appellant)
4. Booth, Courtney C. (attorney for the Plaintiff-Appellant)
5. Butler, Alan J. (attorney for *Amicus Curiae* EPIC)
6. Cable News Network, Inc. (Defendant-Appellee)
7. Cameron, Clinton E. (attorney for Defendant-Appellee)
8. CNN Interactive Group, Inc. (Defendant-Appellee) (wholly owned subsidiary of Cable News Network, Inc.)
9. Electronic Privacy Information Center (EPIC) (*Amicus Curiae*)
10. Historic TW Inc. (parent company of Turner Broadcasting System, Inc.)
11. Edelson, Jay (attorney for Plaintiff-Appellant)
12. Frankel, Jonathan S. (attorney for Defendants-Appellees)
13. Jordon, Jennifer Auer (attorney for Plaintiff-Appellant)
14. Landis, Jeffrey G. (attorney for Defendants-Appellees)

15. Lamberth, James A. (attorney for Defendants-Appellees)
16. Larry. James D. (attorney for Plaintiff-Appellant)
17. Lawson, J. Aaron (attorney for Plaintiff-Appellant)
18. Perlstadt, Roger (attorney for Plaintiff-Appellant)
19. Richman, Benjamin H. (attorney for Plaintiff-Appellant)
20. Ross, Hon. Eleanor L. (presiding district court judge)
21. Rotenberg, Marc (attorney for *Amicus Curiae* EPIC)
22. Sommer, Jacob A. (attorney for Defendants-Appellees)
23. Thomson, Aimee D. (attorney for *Amicus Curiae* EPIC)
24. Time Warner, Inc. (NYSE:TWX) (parent company of Historic TX Inc.)
25. Turner Broadcasting System, Inc. (parent company of Defendants-Appellees)
26. Zwillinger, Marc J. (attorney for Defendants-Appellees)

EPIC is a District of Columbia corporation with no parent corporation. No publicly held company owns 10 percent or more of EPIC stock. To the best of EPIC's knowledge, no person or entity holds 10 percent or more of Time Warner Inc.'s (NYSE:TWX) outstanding common stock.

Dated: July 22, 2016

Respectfully submitted,

/s/ Alan Butler

MARC ROTENBERG
ALAN BUTLER
AIMEE THOMSON
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave., N.W., Suite 200
Washington, D.C. 20009
Tel: (202) 483-1140
Fax: (202) 483-1248

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Other Authorities

STATEMENT OF THE ISSUES

1. Does a unique persistent identifier, such as a mobile phone's Media Access Control ("MAC") address, constitute personally identifiable information ("PII") under the Video Privacy Protection Act ("VPPA")?

2. Does the download and use of a "free" mobile application create a consumer relationship between the user and the video service provider under the VPPA?

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC")[2] is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC has written extensively on the Video Privacy Protection Act and on the privacy implications of the collection, storage, and disclosure of sensitive consumer information. Mot. for Leave to File Amicus Br.

SUMMARY OF ARGUMENT

Congress enacted the Video Privacy Protection Act ("VPPA") to protect the personal consumer information obtained by businesses that offer video services. Congress accomplished this by prohibiting the disclosure of the personal

---

[1] In accordance with FRAP Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC IPIOP clerks Eva Gloster and Ari Lipsitz assisted with the preparation of this brief.

information obtained except in certain narrow circumstances set out in the statute. At the time of enactment, Congress covered every circumstance by which a video service provider could obtain personal information, and construed "personal information" broadly to encompass the various ways that identifiers and elements of a person's identity could be linked to an actual individual.

The lower court got it exactly backwards when it found that techniques linking online transactions to particular individuals were not "personally identifiable information" ("PII") under the VPPA. The court also misunderstood the purpose and scope of the Act when it determined that individuals who obtain videos by using a mobile app offered by a video service provider were not "consumers" under the VPPA.

In the Act, Congress purposefully defined PII broadly to include all information that links a video transaction to a particular person. The lower court is simply incorrect that the unique identifiers at issue in this case are not "tied to an actual person." A name, such as "Ryan Perry," is a less useful way to identify a person than the unique serial numbers tied to a person's cell phone. Moreover, Congress intended the term "consumer" to capture all transactions that would enable a company to collect personal data from those using its service. By excluding a core group of consumers—mobile app users—from VPPA protection, the lower court ignores the premise of the law.

ARGUMENT

The Video Privacy Protection Act of 1988 ("VPPA"), 18 U.S.C. § 2710 (2014), is a quintessential federal privacy statute. The law ensures that consumers can "maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers." S. Rep. No. 100-599, at 8 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342. The VPPA prohibits the disclosure of "personally identifiable information concerning any customer" of a video service provider (or provider of other "similar audio visual materials"), except under certain limited circumstances. § 2710(b)(1); *see The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 5 (2012) (statement of Marc Rotenberg, Executive Director, EPIC)[3] [hereinafter Rotenberg Testimony] ("The law creates narrow exceptions that permit disclosure in certain well-defined circumstances.").

Congress enacted the VPPA with a clear purpose: "to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials." Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710). The Act was introduced after a journalist obtained a list of the video rentals made by the family of Supreme Court nominee Robert Bork, and published

[3] https://epic.org/privacy/vppa/EPIC-Senate-VPPA-Testimony.pdf.

an article commenting on the Borks' movie viewing habits. S. Rep. No. 100-599, at 5; *see* Michael Dolan, *Borking Around*, New Republic (Dec. 20, 2012).[4] Deeply bothered by this invasion of privacy, Congress enacted the VPPA to "prohibit[] video tape service providers from disclosing personally identifiable information except in narrow and clearly defined circumstances." S. Rep. No. 100-599, at 8.

As the bill's original sponsor explained in his introductory floor statement, a "person maintains a privacy interest in the *transactional information* about his or her personal activities. The disclosure of this information should only be permissible under well-defined circumstances." 134 Cong. Rec. 10260 (1988) (statement of Sen. Leahy) (emphasis added). Congress intended the Act to help "define the right of privacy by prohibiting unauthorized disclosure of personal information" by video service providers and to "give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives." S. Rep. No. 100-599 at 6.

Congress intentionally used broad language so that the Act would account for the development of new technologies and services and impose the same privacy standards on companies that would collect and use personal data in the future. VPPA is "technology neutral, setting out rights and responsibilities associated with

[4] https://newrepublic.com/article/111331/robert-bork-dead-video-rental-records-story-sparked-privacy-laws.

the collection and use of personal data that applied regardless of the method employed to deliver video services." Rotenberg Testimony, *supra*, at 12.

To ensure that consumers could hold a company accountable when it disclosed consumer viewing records without consent, Congress explicitly provided for a private right of action. §§ 2710(b)(1), (c); S. Rep. No. 100-599, at 8 ("The civil remedies section puts teeth into the legislation, ensuring that the law will be enforced by individuals who suffer as the result of unauthorized disclosures.").[5] Congress also provided for statutory damages to ensure adequate relief for consumers who suffer privacy invasions. § 2710(c)(2)(A); S. Rep. No. 100-599, at 8 ("Statutory damages are necessary to remedy the intangible harm caused by privacy intrusions.").

I. Unique persistent identifiers, such as MAC addresses, are personally identifiable information under the VPPA.

Congress enacted the VPPA "to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials." Pub. L. No. 100-618, 102 Stat. 3195. The text of the VPPA reflects this purpose, and was drafted in broad language to account for future technological and industry

[5] Plaintiffs have standing to bring suit in consumer privacy cases such as this one, where they have alleged that the defendant's improper disclosure of their personal information constitutes a concrete, particularized, and actual invasion of their legal rights as defined by federal privacy law. *See Spokeo, Inc. v. Robins*, 578 U.S. ___, 136 S. Ct. 1540, 1549 (2016).

developments. In particular, the key statutory term "personally identifiable information" was given a broad definition to ensure that the privacy protections would apply regardless of the type of personal data collected.

The statute specifies that "the term 'personally identifiable information' *includes* information which identifies a person as having requested or obtained specific video materials or services." § 2710(a)(3) (emphasis added). Congress used "the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information." S. Rep. No. 100-599, at 12. As the First Circuit recently observed, "PII is not limited to information that explicitly names a person." *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016). Instead, "personally identifiable information is intended to be transaction-oriented." S. Rep. No. 100-599, at 12. In other words, PII under the VPPA is "information that identifies a particular person as having engaged in a specific transaction with a video tape service provider." *Id.*

Despite Congress's clear focus on identifying a "particular person," some courts have misconstrued the VPPA to require the identification of a person by *name*. *See, e.g.*, *Robinson v. Disney Online*, No. 14-4146, 2015 WL 6161284, at *7 (S.D.N.Y. Oct. 20, 2015) (citing *In re Hulu Privacy Litig.*, No. 11-03764, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014), for the proposition that a "Facebook ID" is PII because it is "equivalent to a name—it stands in for a specific

person, unlike a device identifier"). But the statute does not define PII in terms of its relationship to a name; it defines PII in terms of the ability to *uniquely identify an individual*. In fact, a close reading of the statute makes clear that a "name" is necessarily a subset of a larger category of personally identifiable information. Subsection 2710(b)(2) describes several circumstances in which a video service provider "may disclose personally identifiable information" to others. However, the marketing circumstance set out in section 2710(b)(2)(D) permits the disclosure of "solely" the "names and addresses of consumers." This is the only place in the Act where the term "name" occurs, making it clear that a name is necessarily a subset of the larger category of PII data that might otherwise be disclosed.

Even courts that have improperly narrowed the definition of PII recognize that a name is just one type of PII. *See In re Nickelodeon Consumer Privacy Litig.*, No. 15-1441, 2016 WL 3513782, at *15 (3d Cir. June 27, 2016) (recognizing names, telephone numbers, physical addresses, and social security numbers as PII). But a name is not an even particularly good way to uniquely identify an individual. There are, for example, 425 people in the United States named "Ryan Perry." HowManyOfMe.com.[6] The Plaintiff in this case can be more uniquely identified by other forms of PII: for example, no one else shares his Social Security Number and no one else shares his smartphone Media Access Control ("MAC") address.

[6] http://howmanyofme.com/search/.

These are unique, persistent identifiers that clearly meet the definition of PII under the VPPA when collected in connection with a video viewing transaction.

As Professor Jerry Kang explains in his analysis of the collection and use of personally identifiable information by Internet firms, identifiable information is linked to a *person*, not a person's name. A name is only one kind of personally identifiable information, and PII need not be akin to a name. Information can be identifiable when it "describes a relationship between the information and a person, namely that the information—whether sensitive or trivial—is somehow identifiable to an individual." Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1207 (1998). Information can be "identifiable" to a person in one of three ways: (1) authorship, (2) description, or (3) instrumental mapping. *Id*. First, information that an individual creates and claims authorship over is identifiable. *Id.* Second, information that "could describe the individual in some manner," including characteristics like age and sex, is also identifiable. *Id.* Finally, unique, persistent identifiers (such as Social Security Numbers, usernames, MAC addresses, and unique device addresses) that can be used to map an individual's interactions with an institution over time are also identifiable. *Id*. All three of these categories link information to a person—i.e., *identify* that person.

Moreover, the core concept of PII is that the data does identify *or could identify* a particular individual. Congress purposefully chose the phrase "personally identifi*able* information" instead of "personally identify*ing* information" to make this clear. *See* § 2710(a)(3). Federal privacy laws routinely define PII to include information that either identifies or *could identify* an actual individual. *E.g.*, California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575–22579 (2014) (including information that "permits the physical or online contacting of a specific individual"); E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (including both "direct" and "indirect" identifiers); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012) (including "persistent identifiers that can be used to recognize a user over time and across different Web sites or online services").

In order to determine whether a certain type of record constitutes PII under the statute, the court must first consider whether that information is linked to a "specific [video] transaction"; for example, "whether a person patronized a [provider] at a particular time or on a particular date." S. Rep. No. 100-599 at 12; *see* § 2710(a)(3). If the court finds that the information disclosed links a particular customer to a specific transaction, *see* S. Rep. No. 100-599 at 7, then that information should be considered PII unless it cannot be traced to a particular person.

A. Unique device identifiers are like Social Security Numbers: they are used to link a particular transaction to a unique individual.

The court below simply did not understand the significance of the MAC address used by the service provider to track the activity of the customer to whom it was providing a service. Order 8–9 (finding that a persistent identifier does not constitute PII because it is not "tied to an actual person"). These numbers, assigned to unique devices, are used to track the activities of the individuals using those devices. For example, if a man named John Doe uses the same device to watch videos, browse the news, and order clothes online, then his device identifier can be easily "tied" to his activities over time. Because John Doe owns and uses the device, John Doe the *person* has been linked to specific video transactions, even if his name is absent.

Congress and the courts have recognized that Social Security Numbers ("SSNs"), are "personally identifiable" information. Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909. But the Internet context, unique persistent identifiers such as MAC addresses are a far more robust identifier of particular individuals. MAC addresses make it even easier to track multiple transactions across many services. A device identifier or MAC address is "a series of 12 characters usually in the form xx-xx-xx- xx-xx-xx and is burned into the hardware of a network card." Deepak Gupta et al., *Media Access Control (MAC) Spoofing*

and its Countermeasures, 2 Int'l J. Recent Trends in Eng'g 17, 17 (Nov. 2009).[7] The Institute of Electrical and Electronic Engineers maintains the protocol and registry to ensure that all "MAC addresses and protocol identifiers will be universally unique." IEEE, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, at 20 (2002)[8].

Each device associated with a distinct point of attachment to a local-area network has its own unique MAC address. *Id.* at 22. For example, one computer with several different network connections would have several different MAC addresses. Yet all of the MAC addresses would uniquely identify that computer, and would connect the owner of that computer to her activities online. This enables the company to target advertising and otherwise influence the content delivered to those users by the websites they visit. Laura J. Bowman, *Pulling Back the Curtain: Online Consumer Tracking*, 7:3 I/S: J.L. & Pol'y for Info. Soc'y 718, 721 (2012).[9]

MAC addresses, like IP addresses and other unique, persistent identifiers, "can be used to recognize a user over time and across different websites or online services." FTC, *Complying with COPPA: Frequently Asked Questions* (2015).[10] No two devices share the same MAC address. WiFi interfaces are "periodically

---

[7] http://ijrte.academypublisher.com/vol02/no04/ijrte02041721.pdf.
[8] http://www.ieee802.org/secmail/pdfocSP2xXA6d.pdf.
[9] http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Bowman.Final_.pdf.
[10] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

broadcasting frames containing their MAC address," even when the device is disconnected from a network. Mathieu Cunche, *I Know Your MAC Address: Targeted Tracking of Individual Using Wi-Fi*, Int'l Symp. on Res. in Grey-Hat Hacking (Nov. 2013).[11] As a result, a WiFi-enabled device acts as an "actual wireless beacon" of a device's unique identifier. *Id.* This means that wireless devices periodically broadcast their unique, persistent identifiers in such a way that any nearby device could recognize them. *Id.*

In many cases a name would be insufficient, without more, to link a transaction to a specific individual. For example, the name "Ryan Perry" is insufficient on its own to identify which of the 425 Ryan Perrys in the United States brought this lawsuit. But that does not mean that names are not personally *identifiable* information; all courts and parties agree that they are. Names, when combined with a specific home address or account number, might provide an even more reliable way identify a specific individual. But a unique, persistent identifier such as a device's MAC address is a much better identifier than a name. For the purposes of PII, a MAC address is more like a telephone number—a numeric identifier uniquely linked to a particular individual. These device identifiers are designed to be truly unique and easy to catalog, and therefore can be used to

[11] https://hal.archives-ouvertes.fr/hal-00858324.

"identif[y] a particular person as having engaged in a specific transaction." S. Rep. No. 100-599 at 12; *see Yershov*, 820 F.3d at 489.

Even information that may appear "anonymous," such as a string of numbers, could be used to link an individual to specific transactions. Social Security Numbers, like MAC addresses and other unique, persistent identifiers, consist of a string of semi-random numbers. Carolyn Puckett, *The Story of the Social Security Number*, 69 Soc. Security Bulletin 55, 57 (2009).[12] Yet courts routinely acknowledge that SSNs are PII under the VPPA. *See*, *e.g.*, *In re Nickelodeon Consumer Privacy Litig.*, 2016 WL 3513782, at *15 (finding that PII under the VPPA includes "pieces of information, like social security numbers, which are associated with individual persons but might not be easily matched to such persons without consulting another entity, such as a credit reporting agency or government bureau"). Even the United States acknowledges that PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as . . . Social Security number." Gov't Accountability Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (May 2008).[13] The same is true of "a telephone number or a physical address, which may

[12] https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[13] http://www.gao.gov/new.items/d08536.pdf.

not by themselves identify a particular person but from which it would likely be possible to identify a person by consulting publicly available sources, such as a phone book or property records." *In re Nickelodeon Consumer Privacy Litig.*, 2016 WL 3513782, at *15. Similarly, GPS coordinates are strings of numbers that mean nothing without access to a map, but can identify a person's unique residence with greater specificity than an address.[14] *See id.* at *20.

Unique persistent identifiers such as Ryan Perry's MAC address are unique to Plaintiff Ryan Perry—even more uniquely identifying than Ryan Perry's name, which is shared by 424 other individuals in the United States. Oddly, the lower court concluded that the disclosure of the ambiguous name "Ryan Perry" was covered under the federal privacy law, when it was the disclosure of the unique identifier associated with Plaintiff Ryan Perry that constituted the far clearer privacy harm, much like disclosing a SSN or telephone number would.

B. Internet companies use unique, persistent identifiers to link specific Internet users to video transactions.

Like many Internet advertising and media companies, CNN collects a wide range of information about its users, including the unique persistent identifiers at issue in this case. Companies such as CNN then use this data to identify individual users and track their behavior over time and across different websites. *See*

[14] For example, an address could only lead someone to an apartment building; GPS coordinates could place a person inside a unique apartment.

Rotenberg Testimony, *supra*, at 8 ("Every computer connected to the Internet receives an IP address that is logged by web servers as the user browses the Internet. These logs allow companies to record a trail of the user's online activity. Companies engage in extensive tracking and data collection about the online activities on consumers."). In other words, CNN is trying to obtain the benefits of PII for logging user transactions while ignoring the legal obligations associated with the collection and use of PII under the federal law. But is no distinction: Whenever companies collect unique persistent identifiers in connection with data about the videos its users are watching, that data is PII under the VPPA, unless it can be demonstrated that the identifier cannot be linked to a particular individual.

In its privacy policy, CNN explains that it collects data for the purpose of tracking users. CNN collects a user's "device identifiers (such as an Apple IDFA or an Android Advertising ID)," "network or Internet protocol address," "device settings," "browser settings," "location information," as well as the information about the "type of browser you are using," the "type of operating system you are using," and "the content and advertisements you have accessed, seen, forwarded and/or clicked on." CNN, *CNN Privacy Statement.*[15] This enables the company to "*customize or personalize* ads, offers and content made available to you based on your visits to and/or usage of the Services or other online or mobile websites,

[15] http://www.cnn.com/privacy.

applications, platforms or services, and analyze the performance of those ads, offers and content, as well as *your interaction with them*." *Id.* (emphasis added).

Data aggregators such as Bango, with which CNN shared Mr. Perry's unique persistent identifiers and video viewing history, also use the data at issue in this case to identify and track users. Bango creates a "Bango User ID" for each user that "on its own[,] is not personally identifiable." Bango, *Bango Privacy Policy*.[16] But Bango's claim is contradicted by its very own policy. The User ID is a "unique identification number" that is "created from cookies, browser header information, IP addresses and information supplied by Bango partners," and is "*linked to your device* (manufacturer and model), mobile network operator or mobile virtual network operator, current connection and operator's country." *Id.* (emphasis added). Bango therefore uses unique persistent identifiers, *linked to the user's device*, to uniquely identify users.

Given these statements regarding CNN and Bango's collection and use of customer data, it is clear that persistent identifiers, uniquely tied to the user's device, meet the definition of PII under the VPPA. The companies collect and use these very identifiers to track users viewing habits and other activities. This linkage of the individual user's device with her viewing habits *is* the act of identification under the federal privacy law.

[16] http://bango.com/privacy/.

II. Users of mobile apps are "consumers" under the federal privacy law because they provide valuable personal data to video service providers.

The VPPA prohibits a video service provider from knowingly disclosing the PII concerning any "consumer" of its service, which the Act defines as any "renter, purchaser, or subscriber of goods or services from a video tape service provider." §§ 2710(a)(1), (b)(1); *see* Allison Grande, *Mich. Court Further Curbs Streaming Privacy Laws In Pandora*, Law360 (July 11, 2016)[17] ("'A relationship between the company and customer is established by virtue of the consideration that Pandora obtained: the personal data of Peter Deacon, which it then disclosed for further commercial benefit,' [EPIC Executive Director Marc] Rotenberg said."). Congress regulates the collection of PII "that identifies a particular person as having engaged in a specific *transaction* with a video tape service provider." S. Rep. No. 100-599 at 12 (emphasis added). The Act is not focused on the purchase and sale of video services, but rather the "transactions" associated with the delivery of the video service. The regulated entity is one that engages in the "rental, sale, or *delivery*" of videos. § 2710(a)(4) (emphasis added). If a video service provider subsequently discloses a consumer's PII for reasons not permitted in the statute, then it are liable under the VPPA. § 2710(b)(1).

[17] http://www.law360.com/articles/816102/mich-court-further-curbs-streaming-privacy-laws-in-pandora.

In 2015, this Court expressed doubt that users of "free" mobile apps qualified as "consumers" under the Act. *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1257–58 (11th Cir. 2015).[18] The Court said that subscriber relationships require an "ongoing commitment or relationship" between the plaintiff and defendant. *Id.* at 1257. The Court was skeptical that downloading and using a mobile app to watch video content—"without more"—would make a user a consumer of video services. *Id.* at 1258. But the *Ellis* Court's decision was wrong because it did not understand that the obligations of the Act are triggered when the video service provider obtains personal information from the user. This is precisely the point of the Act. As Senator Leahy said, a "person maintains a privacy interest in the *transactional information* about his or her personal activities. The disclosure of this information should only be permissible under well-defined circumstances." 134 Cong. Rec. 10260 (statement of Sen. Leahy) (emphasis added).

Whether a user streams a video under a subscription plan or under an ad-supported option, that user is still a "consumer" of the video service. Mobile apps have simply created another way for video service providers to obtain the personal data of users. In fact, the privacy claim is stronger in the ad-supported model than

[18] A mobile application, or "app," is a generally a "small, individual software unit[]" that is "designed to run on a mobile device, such as a smartphone or tablet computer." Technopoedia, *Mobile Application (Mobile App)* (2016), https://www.techopedia.com/definition/2953/mobile-application-mobile-app.

in the subscription model: the consideration provided for the service is not a subscription payment, but rather the personal data of the user. Because the core purpose of the video privacy law is the protection of the personal data obtained by a service provider, the privacy interest is clearly greater for Mr. Perry here than it would otherwise be with a subscription model.

A. Mobile apps are not equivalent to browser bookmarks.

Contrary to this Court's conclusion in *Ellis*, mobile apps are not like bookmarks. *Ellis*, 803 F.3d at 1257. Browser bookmarks do not create any fiduciary relationship between a consumer and a company. There is no transfer of user data to the firm. Mobile apps generate value for the company: the entire business model is to collect the personal data of the user.

"Bookmarking" is an organizational tool that has been present within Internet browsers since 1993. *See* Marc Andreessen, *New X-Based Information Systems Browser Available*, comp.infosystems (Feb. 16, 1993).[19] Bookmarks enable quick access to a set of webpages predetermined by a browser user. They are functionally identical to a saved series of hyperlinks. *See generally* APA Style, *What a Tangled Web: Website Versus Web Page* (Oct. 8, 2014) ("A *web page* is a computer file on the web, displayed on a monitor or mobile device, which could provide text, pictures, or other forms of data. A *website* consists of a collection of

[19] https://groups.google.com/forum/#!topic/comp.infosystems/855ZNG7mvI0.

web pages provided by one person or organization; all of the pages trace back to a common Uniform Resource Locator (URL) and are usually hyperlinked to each other.").[20]

Historically, bookmarks were saved locally on a computer's hard drive within the user's browser files. *See, e.g.*, Microsoft, *Netscape Bookmark File Format*.[21] Newer browsers can save bookmarks to a browser manufacturer's cloud server, which permits users to access their lists from any computer. *See, e.g.*, Google, *Sync Chrome Data Across Devices*.[22] But the basic function of a browser bookmark has not changed significantly since 1993. A bookmark simply allows an Internet user to quickly access a specific webpage. A bookmark is one of the rare Internet tools that nearly perfectly approximates its physical analog: click on the bookmark, and find your page.

A mobile app, by contrast, necessarily involves the transfer of the user's personal data to the app provider. An app is a fully-fledged program running on the operating system of a smartphone. Technopedia, *Mobile Application (Mobile App)*, *supra*. Apps are downloaded via a centralized distribution platform, such as the Apple "App Store." Modern smartphone apps have become widely used since their

[20] http://blog.apastyle.org/apastyle/2014/10/what-a-tangled-web-website-versus-webpage.html.
[21] https://msdn.microsoft.com/en-us/library/aa753582 (last visited July 11, 2016).
[22] https://support.google.com/chrome/answer/165139 (last visited July 11, 2016).

introduction in the Apple App Store in 2008. Jenna Wortham, *Apple's Game Changer, Downloading Now*, N.Y. Times (Dec. 5, 2009)[23] ("Thanks in large part to the iPhone, introduced in 2007, and the App Store, which opened its doors last year, smartphones have become the Swiss Army knives of the digital age.").

The crucial difference between mobile apps and browser bookmarks is the access to user data. A bookmark does not provide a website with any personal data about the user—the bookmark is created and maintained by the user on her own browser. Mobile apps, by contrast, are controlled by and send data to their providers. Under this model, companies collect a great deal of valuable personal information about consumers. *See* John Herrman, *The Next Internet Is TV*, Awl (Feb. 5, 2015)[24] (suggesting that major publishers like CNN are moving away from free websites toward television-like "channels" within mobile apps); *see generally* Dave Sikora, *How Mobile Apps Are Reviving Branded Walled Gardens*, Mobile Marketer (Sep. 23, 2013)[25] ("This walled garden is a closed-loop system for engagement, loyalty, customer service and payments that begins with opening the mobile app and ends with closing the mobile app.").

[23] http://www.nytimes.com/2009/12/06/technology/06apps.html.
[24] https://theawl.com/the-next-internet-is-tv-a0d57c37349#.becooac9w.
[25] http://www.mobilemarketer.com/cms/opinion/columns/16208.html.

B. Users of "free" apps are consumers of services because the app company obtains consideration from the user in the form of personal data.

Apps sell audiences, not advertising. *See* Jeff Sonderman, *Advertisers Buy Audiences, Not Publications or Platforms, and Data is the Key*, Am. Press Inst. (June 10, 2014).[26] App developers obtain the personal data of users, which is the essential bargain of the app economy and the reason that users of these apps constitute "consumers" under the VPPA. *See Yershov*, 820 F.3d at 489 ("While he paid no money, access was not free of a commitment to provide consideration in the form of that information, which was of value to Gannett."). This is not to say that every mobile video app collecting user data violates the VPPA; an app developer only violates the Act if they disclose the user's PII in contravention of the Act. § 2710(b)(1). But the users that provide their personal data to mobile apps must fall under the scope of the Act because they are most certainly consumers.

Facing a similar case, the First Circuit recently found that such users were "consumers" under the federal privacy law. *Yershov*, 820 F.3d at 489. Whether or not Mr. Perry paid money to CNN, he was a consumer of CNN's video services. Other courts have found that a user's access to free streaming video services through a web browser gives rise to a "consumer" relationship under the VPPA.

[26] https://www.americanpressinstitute.org/publications/reports/white-papers/advertisers-audiences-data/.

See, e.g., *In re Hulu Privacy Litig.*, No. 11-03764, 2012 WL 3282960 (N.D. Cal. Aug. 12, 2012).

The Court also doubted that downloading a mobile app could create a "subscriber" relationship because it did not involve registration. *Ellis*, 803 F.3d at 1257; *cf. In re: Hulu Privacy Litig.*, 2012 WL 3282960 at *8. But there is no need for a provider to require app users to register—the company can already collect their data based on their downloading and use of the app. Even if users do not type in their names or create passwords, the act of downloading, "without more," has registered them in the company's advertising database. *See, e.g.*, Google, *Target Mobile Apps With IDFA or AAID*[27] ("Every iOS device comes with an identifier that allows developers and marketers to track activity for advertising purposes.").

This practice means a user must be understood as a "consumer" regardless of the ease of deletion. In *Ellis*, the Court theorized that because a user could delete an app, she should not be considered a consumer of the app provider. *Ellis*, 803 F.3d at 1257. But a Blockbuster consumer is no less a consumer under the VPPA because she could close her account or choose not to frequent the store. Even if a user deletes a mobile app, the transactional data about that user's video viewing

[27] https://support.google.com/adxbuyer/answer/3221407?hl=en (last visited June 27, 2016). This is only one implementation of the set of unique identifiers collected by mobile apps.

habits is still in the possession of the video service provider. It is the collection and use of the personal information that is the central concern of the VPPA.

Collecting consumer personal data is the central reason for offering "free" video services through a mobile app. As a user whose personal data was obtained by a mobile app offering video service, Mr. Perry is a "consumer" under the federal video privacy law.

* * *

In 1988, Congress established clear limits on the collection and use of personal data by companies providing video services. The passage of time has only made clearer the importance of this federal privacy law.

CONCLUSION

EPIC respectfully requests that this Court vacate the district court's opinion.

Dated: July 22, 2016

Respectfully submitted,

/s/ Alan Butler

MARC ROTENBERG
ALAN BUTLER
AIMEE THOMSON
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave., N.W., Suite 200
Washington, D.C. 20009
Tel: (202) 483-1140
Fax: (202) 483-1248

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because this brief contains 5,381 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief has been prepared in a proportionally spaced typeface, 14-point Times New Roman, using Microsoft Word for Mac 2011.

/s/ Alan Butler

Dated: July 22, 2016 ALAN BUTLER

CERTIFICATE OF SERVICE

I hereby certify that on July 22, 2016, I electronically filed the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Appellant with the Clerk of the Court of the United States Court of Appeals for the Eleventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and will be served via the CM/ECF system.

/s/ Alan Butler

Dated: July 22, 2016 ALAN BUTLER