IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA, ATLANTA DIVISION

MARK ELLIS, individually and on behalf of all others similarly situated, *Plaintiff*, *v.* THE CARTOON NETWORK, INC., a Delaware corporation, *Defendant*.	Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Mark Ellis ("Ellis") brings this Class Action Complaint and Demand for Jury Trial ("Complaint") against The Cartoon Network, Inc., ("Cartoon Network") to put an end to its unlawful practice of disclosing its users' sensitive information, and to obtain redress for such conduct. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys:

NATURE OF THE ACTION

1. Cartoon Network produces a variety of (mostly animated) television programming. Although perhaps best known for its eponymously named television

channel, Cartoon Network also offers media to consumers via other mediums, including on mobile devices (such as Android[1] smartphones) through its proprietary mobile software application, the Cartoon Network App (the "CN App").

2. Unbeknownst to its users, each time that a person views video clips or watches television shows using the CN App on their Android, Cartoon Network discloses their personally identifiable information—including a record of every video clip or television showed viewed by the user (collectively, "PII")—to unrelated third parties. In addition to demonstrating a brazen disregard for its users' privacy rights, Cartoon Network's actions also violate the Video Privacy Protection Act, 18 U.S.C. § 2710 ("VPPA"), which prohibits companies from disclosing their customers' video viewing records to third parties without express written consent.

3. Cartoon Network's violation of the VPPA is particularly flagrant here, as it programmed the CN App to submit users' PII to a third party web data analytics company. The business models of such "big data" companies center on the collection of disparate pieces of uniquely identifying information and online

---

[1] Android is a mobile device operating system developed by Google, Inc. Many smartphones, including certain devices manufactured by HTC Corp. and the Samsung Group, utilize the Android operating system.

behavioral data about individual consumers, which they then compile to form comprehensive profiles about a person's entire digital life. These profiles can then be used for targeted advertising, sold as a commodity to other data brokers, or both.

4. In an era when the collection and monetization of consumer data proliferates on an unprecedented scale, it's important that companies are held accountable for the exploitation of their users' sensitive information. Cartoon Network chose to disregard Plaintiff's and thousands of other users' statutorily protected privacy rights by releasing their sensitive data into the marketplace. Under the VPPA, that makes Cartoon Network liable.

PARTIES

5. Plaintiff Mark Ellis is a natural person and citizen of the State of North Carolina.

6. Defendant The Cartoon Network, Inc., is a corporation incorporated in and existing under the laws of the State of Delaware, with its headquarters and principal place of business located at 1015 Techwood Drive NW, Atlanta, Georgia 30318. Defendant The Cartoon Network, Inc. conducts business throughout this District, the State of Georgia, and the United States.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 as this action arises under the VPPA. This Court has personal jurisdiction over Defendant because its headquarters are located in this District, it conducts business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

8. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

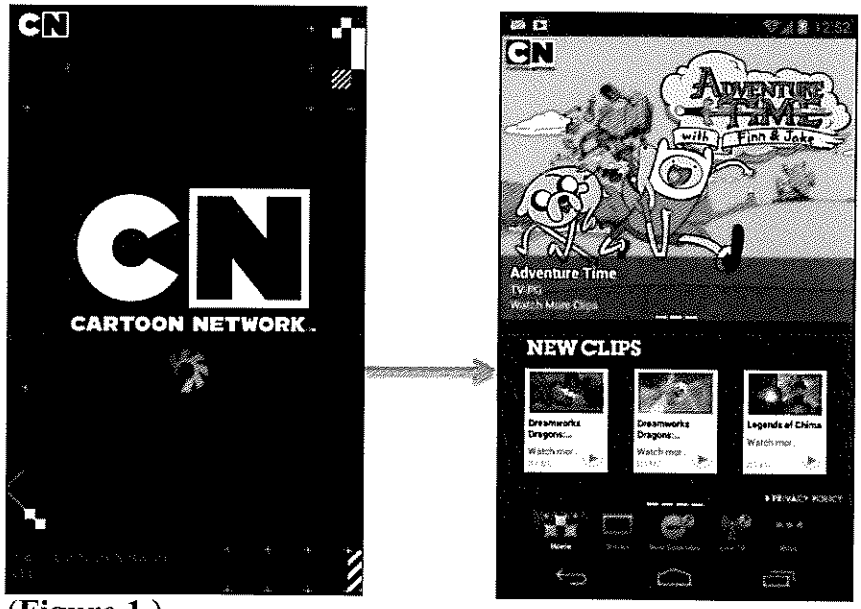
FACTUAL BACKGROUND

I. Cartoon Network Programmed the CN App to Transmit Its Users' PII and Video Viewing Activity to a Third Party Analytics Company Without Their Consent.

9. The CN App is a mobile application that allows consumers to access Cartoon Network's programming and "see videos from hit Cartoon Network shows like: Adventure Time, Regular Show, Ben 10, Ninjago, The Looney Tunes Show, The Amazing World of Gumball, MAD and many more." Cartoon Network also says that the CN App lets users "Watch our library of video clips, or log in with your TV provider info to get even more benefits like: Watch live TV! Stream

Cartoon Network directly to your device."[2]

10. To install the application on an Android, users must visit the Google Play Store, the online digital media platform operated by Google. Once downloaded and installed, and upon opening the application for the first time, the CN App presents a loading screen and then proceeds to a main home screen. (*See* Figure 1, showing the CN App when first opened).



(Figure 1.)

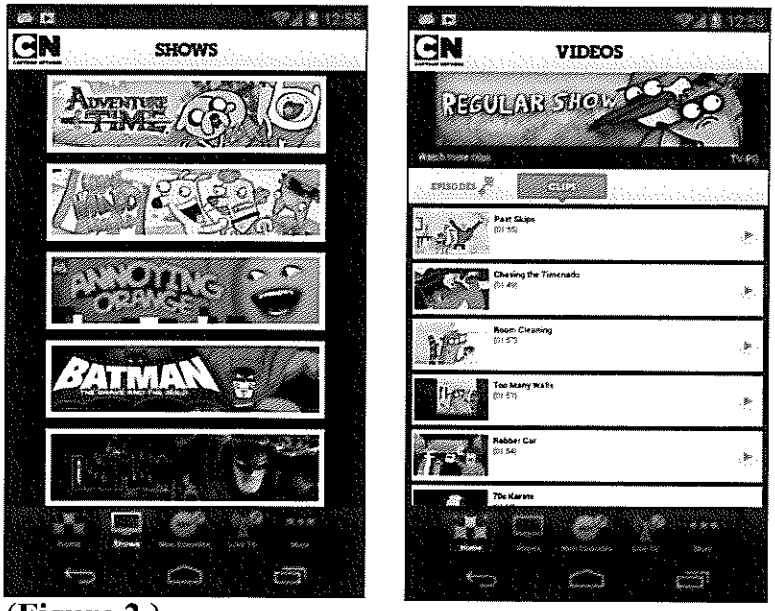
11. At no time during this process, however, does Cartoon Network seek or obtain the consent of the user to share or otherwise disclose his or her PII to third parties for any purpose.

---

[2] Cartoon Network Video, https://play.google.com/store/apps/details?id=com.turner.cnvideoapp&hl=en (last accessed February 17, 2014).

1. The CN App sends the video viewing activity and uniquely identifying PII of its users to the data analytics company Bango.

12. The CN App is organized into certain sections that are accessible through the software's main user interface (UI). (*See* Figure 2, showing the CN App's user interface). Users may browse around these sections to view video clips and television shows. (*See id.*)



(Figure 2.)

Unbeknownst to its users, however, each time they view video clip or television show, the CN App sends a record of such activities to an unrelated third party data analytics company called Bango.[3] The complete record is sent each time that the

[3] Bango is a data analytics company based in the United Kingdom. The company claims to specialize in tracking individual user behaviors across the

CN App is closed, along with the unique Android ID[4] associated with the user's mobile device.

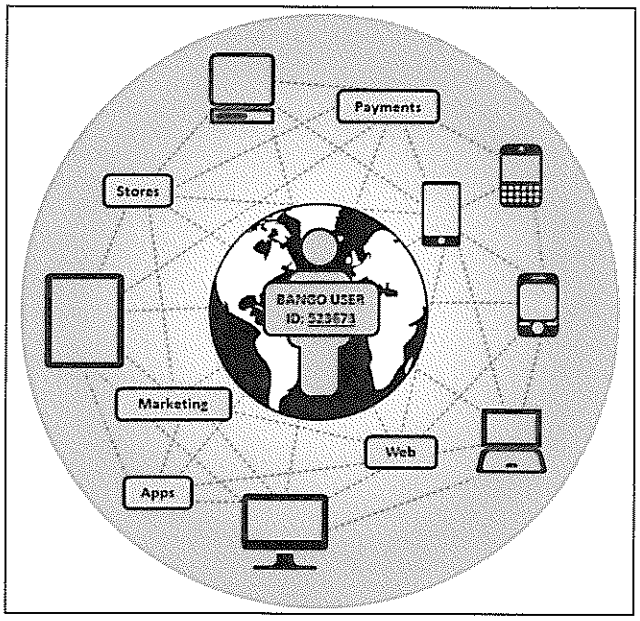
II. Data Analytics Companies Rely on Unique Identifiers Associated with Mobile Devices to Create Digital Dossiers On Consumers and Their Online Behaviors.

13. Today's average consumer uses more than one device to access the Internet to do things like view digital content or make online purchases. This creates challenges for online advertisers and analytics companies. Namely, to gain a broad understanding of a given consumer's behavior across all of the devices that he or she uses, these companies have to find ways to "link" their digital personas. The primary solution has been to use certain unique identifiers to connect the dots.

14. The graphic from Bango's website shown in Figure 3 below provides a simplistic illustration of how this process works:

Internet and mobile applications. Bango boasts that its technology "reveals customer behavior, engagement and loyalty across and between all your websites and apps." (*See* Bango Analytics, http://bango.com/mobile-analytics/ (last accessed February 17, 2014)). To accomplish this, Bango relies on uniquely identifying information about consumers to track their behavior.

[4] 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." Android Developer's Guide, http://developer.android.com/reference/android/provider/Settings.Secure.html#ANDROID_ID (last accessed February 17, 2014).



(Figure 3.)

15. As depicted in Figure 3, the key to successfully tracking an individual's online behavior is to precisely identify the person and link their activities across websites and devices. To do this, Bango relies on, in relevant part, "[o]perator and device manufacturer supplied identity."[5]

16. An example of an "[o]perator and device manufacturer supplied identity" in the mobile computing context is the Android ID. That's because Android IDs are "persistent identifiers," meaning they are unique to a specific device and remain constant for the lifetime of the user's device. In other words, once an Android ID is matched with an individual's identity, it's exceedingly difficult for that person to avoid being tracked via their mobile device—making it

[5] Bango Analytics, http://bango.com/mobile-analytics/ (last accessed February 17, 2014).

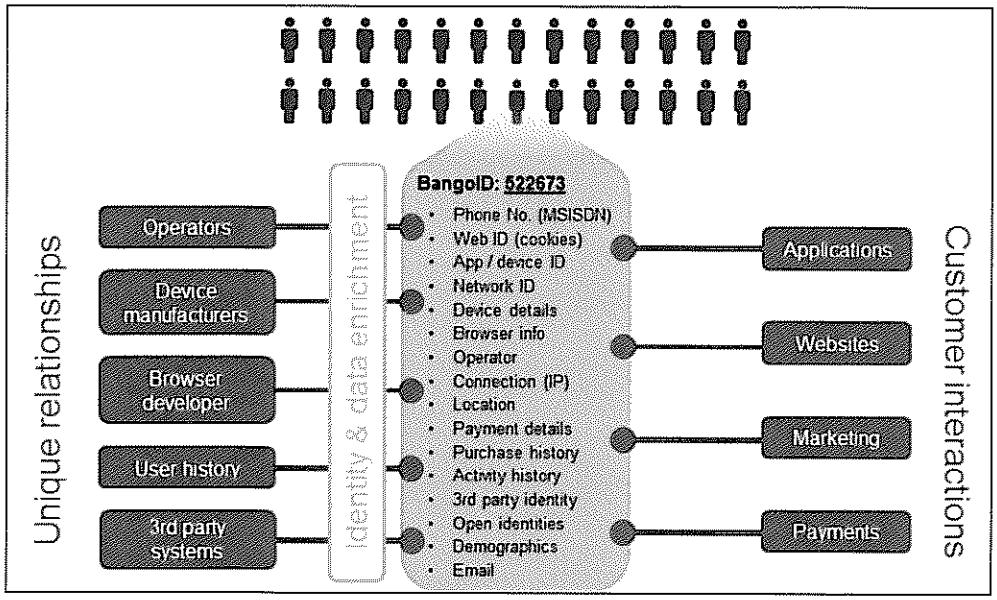
among the most stable and reliable identifiers for a given individual.

1. Bango and other analytics companies maintain massive digital dossiers on consumers.

17. Once a consumer's identity is matched with their device's Android ID, a wealth of extremely precise information can be gleaned about the individual. For instance, mobile applications that transmit an Android ID along with the user's activity within the software provide an intimate look into how people interact with their software, including revealing information such as the games played, articles read, videos viewed, and even detail about the sequence of events in which the user conducted these actions.

18. An excerpt from one of Bango's marketing materials, shown in Figure 4 below, accurately portrays the frightening array of information that feeds into a consumer's digital dossier using data transmitted from sources such as mobile applications:

* * *



(**Figure 4.**)

19. Figure 4 provides insight into the depth of information stored by analytics companies like Bango. Of particular note is that "Applications" shown in top right tab—such as the CN App—assist in the "data enrichment" of a consumer's profile, which includes information like the person's location, phone number, email, purchase history, app activity history, and payment details.

2. Congress investigates mobile apps and third party analytics companies while the NSA uses the same data to profile individuals.

20. The privacy risks associated with collecting and transmitting PII from mobile applications to third parties is no longer just academic musing. Congress is taking notice, and has held subcommittee meetings—including one focusing on "Consumer Privacy and Protection in the Mobile Marketplace"—to address the

issue. During that hearing, Senator John Rockefeller noted that, "these third parties use [consumer data] to target advertising on individuals . . . It is very good business, but it is very cynical. It is an abuse of that power, passing on people's profiles."[6]

21. At the same time, and perhaps most strikingly, classified documents from the National Security Agency (NSA) reported on by the New York Times show that the government agency targets this very information (uniquely identifying data sent from mobile apps) to create detailed profiles on individuals.[7]

22. Despite the controversy surrounding these methods of harvesting and commodifying sensitive consumer data, Cartoon Network chose to disclose nearly every digital movement of its CN App users—including Android IDs—to a third party analytics company.

III. The VPPA's Importance in the Digital Age.

23. When the VPPA was introduced, the late Senator Paul Simon noted that, "[e]very day Americans are forced to provide to businesses and others

---

[6] S. Hrg. 112-289, Consumer Privacy and Protection in the Mobile Marketplace, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg73133/html/CHRG-112shrg73133.htm (last accessed February 17, 2014).

[7] Spy Agencies Scour Phone Apps for Personal Data, http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html#document/p10/a142016 (last accessed February 17, 2014).

personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes." S.Rep. No. 100-599 at 7–8 (1988). Senator Patrick Leahy, one of the original drafters of the VPPA, also remarked that, "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id.* at 8.

24. While these statements rang true in 1988 when the act was passed, the need for legislation like the VPPA in the modern computing era is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized this point, saying that, "[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[8]

25. Likewise, Senator Al Franken summed up the importance of the

---

[8] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/hearings/hearing.cfm?id=f14e6e2889a80b6b53be6d4e412d460f (last accessed February 17, 2014).

VPPA in today's world as follows: "[i]f someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."

IV. Plaintiff Ellis's Experience with the CN App.

26. Starting in early 2013, Plaintiff Ellis downloaded and began using the CN App on his Android to watch video clips.

27. At all times relevant, Ellis never consented, agreed, or otherwise permitted Cartoon Network to disclose his PII to any third party analytics companies.

28. Likewise, Ellis has never been given the opportunity to prevent the CN App from disclosing his PII to third parties.

29. Nevertheless, each time Ellis viewed a video clip using the CN App, Cartoon Network disclosed his PII to third party analytics company Bango.

CLASS ALLEGATIONS

30. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of himself and a Class of similarly situated individuals, defined as follows:

> All persons in the United States used the CN App to watch videos and had their PII transmitted to Bango.

Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entity's current and former employees, officers, and directors, (2) the Judge to whom this case is assigned and the Judge's immediate family, (3) persons who execute and file a timely request for exclusion from the Class, (4) persons who have had their claims in this matter finally adjudicated and/or otherwise released, and (5) the legal representatives, successors, and assigns of any such excluded person.

31. **Numerosity**: The exact number of members of the Class is unknown and is not available to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals. Class members can be easily identified through Defendant's records.

32. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

a) Whether Defendant, through the CN App, unlawfully disclosed and continues to unlawfully disclose its users' personally

identifiable information, including their video viewing records, in violation of 18 U.S.C. § 2710(b);

b) Whether Defendant knowingly violated the VPPA;

c) Whether Defendant disclosed Plaintiff and Class members' personally identifiable information without their consent; and

d) Whether Defendant violated Plaintiff and Class members' right to privacy.

33. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiff and the Class.

34. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

35. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward members of the Class. The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Class are the same, resulting in injury to the Plaintiff and to all of the other members of the Class. Plaintiff and the members of the Class have suffered harm and damages as a result of Defendant's unlawful and wrongful conduct.

36. **Superiority**: This case is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The injuries suffered by the individual members

of the Class are likely to have been relatively small compared to the burden and expense of individual prosecution of the litigation necessitated by Defendant's actions. Absent a class action, it would be difficult, if not impossible, for the individual members of the Class to obtain effective relief from Defendant. Even if members of the Class themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties and the Court and require duplicative consideration of the legal and factual issues presented herein. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

37. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of the Video Privacy Protection Act
(18 U.S.C. § 2710)
(On behalf of Plaintiff and the Class)

38. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

39. Defendant is a "video tape service providers as defined by the VPPA because it "engage[s] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery or prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4), because it provides video (i.e., "similar audio visual materials" under the VPPA's definition) to consumers via its CN App.

40. Plaintiff is a "consumer" as defined by the VPPA because he downloaded, installed, and watched videos using the CN App. 18 U.S.C. § 2710(a)(1). Under the Act, this means that he was a "subscriber" of "goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1).

41. While the CN App was installed on his Android, Plaintiff viewed numerous video clips using the software. On information and belief, during these occasions and on closing the CN App, the software sent Plaintiff's PII—including his phone's Android ID and records of the videos that he viewed—to the third party analytics company Bango.

42. The CN App's transmissions of Plaintiff's PII to Bango constitute "knowing[] disclosures" of Plaintiff's "personally identifiable information" to a person as proscribed by the VPPA. 18 U.S.C. § 2710(a)(1).

43. Under the VPPA, 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). The definition's usage of the word "includes" means that a more expansive reading of the term was expressly contemplated.

44. The National Institute of Standards and Technology (NIST) defines "personally identifiable information" as "any information that can be used to distinguish or trace an individual's identity."[9] As described in detail in Section II above, Plaintiff's PII transmitted to Bango from the CN App can be used to distinguish or trace his identity.

45. At no time did Plaintiff ever provide Cartoon Network with any form of consent—either written other otherwise—to disclose his PII to third parties.

46. Nor were Cartoon Network's disclosures made in the "ordinary course of business" as the term is defined by the VPPA. In particular, the CN App's disclosures to Bango (an analytics company) were not necessary for "debt collection activities, order fulfillment, request processing, [or] the transfer of ownership." 18 U.S.C. § 2710(a)(2).

47. As a result of Defendant's unlawful disclosures, Plaintiff and the

[9] NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (last accessed February 17, 2014).

Class have had their statutorily defined right to privacy violated. Plaintiff seeks an injunction to prohibit Cartoon Network from releasing his and the Class's PII in the future, as well as the maximum statutory and punitive damages available under the VPPA. 18 U.S.C. § 2710(c).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Mark Ellis, on behalf of himself and the Class, respectfully requests that this Court enter an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Mark Ellis as class representative, and appointing his counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate the VPPA, 18 U.S.C. § 2710;

C. Awarding injunctive and other equitable relief as necessary to protect the interests of the Class, including, *inter alia*, an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

D. Awarding damages, including statutory damages of $2,500 per violation, and punitive damages, where applicable, in an amount to be determined at trial pursuant to the VPPA, 18 U.S.C. § 2710(c);

E. Awarding Plaintiff and the Class their reasonable litigation expenses

and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

MARK ELLIS, individually and on behalf of all others similarly situated,

Dated: February 19, 2014

By: /s/Jennifer Auer Jordan
One of Plaintiff's Attorneys

Jennifer Auer Jordan (No. 027857)
jennifer@thejordanfirm.com
THE JORDAN FIRM, LLC
1447 Peachtree Street, N.E., Suite 880
Atlanta, Georgia 30309
Tel: 404.445.8400
Fax: 404.445.8477

LOCAL RULE 5.1 CERTIFICATION

I, Jennifer Auer Jordan, hereby certify that on February 19, 2014, I filed the above and foregoing ***Class Action Complaint and Demand for Jury Trial*** with the Clerk of the Court and that such paper complies with Local Rule 5.1 and was prepared using a typeface of 14 points in Times New Roman.

/s/Jennifer Auer Jordan
Ga. Bar No. 027857)
jennifer@thejordanfirm.com
THE JORDAN FIRM, LLC