IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	)	**C.A. 12-7829 (SRC)(CLW)**
	)	**MDL No. 2443**
	)	
	)	**Judge Stanley R. Chesler**
	)	
	)	**MASTER CONSOLIDATED**
This Document Relates to:	)	**CLASS ACTION COMPLAINT**
	)	
All Actions	)	
	)	

I. INTRODUCTION AND OVERVIEW

1. This class action seeks damages and injunctive relief on behalf of all minor children under the age of 13 in the United States who visited the websites Nick.com, NickJr.com, or NeoPets.com. Defendant Viacom Inc., (hereinafter "Viacom") owns and operates these websites, each of which has a target audience of minor children.

2. Specifically, this case is about Defendant Viacom and Defendant Google Inc.'s (hereinafter "Google") misuse of Internet technologies ("cookies") to disclose compile, store and exploit the video viewing histories and Internet communications of children throughout the United States in contravention of federal and state law. With neither the knowledge nor the consent of their parents, unique and specific electronic identifying information and content about each of these children was accessed, stored, and utilized for commercial purposes.

3. This case is brought to enforce the privacy rights of these children, and to enforce federal and state laws designed to uphold those rights.

II. NATURE OF THE ACTION

4. The named Plaintiffs are minor children under the age of 13 who were registered users of the websites Nick.com, Nickjr.com and NeoPets.com.

5. The Defendants utilized Internet technologies commonly known as "cookies" to track and share the plaintiffs' and putative class members' video-viewing histories on Nick.com, Nickjr.com and NeoPets.com without plaintiffs' informed written consent.

6. The Defendants further utilized these technologies to track plaintiffs' and the putative class members' Internet communications without plaintiffs' authorization or consent.

7. Plaintiffs are informed and believe the Defendants' conduct is systematic and class wide.

8. The Defendants' conduct violated federal and state laws designed to protect the privacy of American citizens, including children. Such conduct gives rise to the following statutory and common law causes-of-action:

a. Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710, et seq.;

b. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq.;

c. Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.;

d. Violation of the California Invasion of Privacy Act, Cal. Penal Code §631(a), et seq.;

e. Violation of the New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq.;

f. Intrusion Upon Seclusion; and

g. Unjust Enrichment.

III. THE PARTIES

A. Plaintiffs

9. Plaintiffs C.A.F., C.T.F., M.P. and T.P. are minor children under the age of 13 who reside in the State of New Jersey. At all relevant times, they have been registered users of the websites Nick.com and/or NickJr.com.

10. Plaintiff L.G. is a minor child under the age of 13 who resides in the State of California. At all relevant times, L.G. has been a registered user of the website Nick.com and/or NickJr.com.

11. Plaintiff T.M. is a minor child under the age of 13 who resides in the State of Illinois. At all relevant times, T.M. has been a registered user of the websites Nick.com, NickJr.com and/or NeoPets.com.

12. Plaintiff N.J. is a minor child under the age of 13 who resides in the State of Missouri. At all relevant times, N.J. has been a registered user of the website Nick.com and/or NickJr.com.

13. Plaintiff A.V. is a minor child under the age of 13, who resides in the State of New York. At all relevant times, A.V. has been a registered user of the website Nick.com and/or NickJr.com.

14. Plaintiff Johnny Doe is a minor child under the age of 13, who resides in the State of Texas. At all relevant times, he has been a registered user of the website Nick.com, NickJr.com and/or NeoPets.com.

15. Plaintiff K.T. is a minor child under the age of 13, who resides in the state of Pennsylvania. At all relevant times, K.T. has been a registered user of the website Nick.com and/or NickJr.com.

B. Defendant Viacom

16. Defendant Viacom, Inc. is a publicly-traded Delaware corporation with headquarters at 515 Broadway, New York, New York 10036. Defendant Viacom does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

17. Defendant Viacom publicly proclaims its Nickelodeon division to be "the number-one entertainment brand for kids."[1]

C. Defendant Google

18. Defendant Google, Inc. is a publicly traded Delaware corporation with headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Defendant Google does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

19. Google has, by design, become the global epicenter of Internet search and browsing activity. Underscoring its vast Internet reach, Google describes its "mission" as "to organize the world's information and make it universally accessible and useful."[2]

IV. JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendants because all Defendants have sufficient minimum contacts with this District in that they all operate businesses with worldwide reach, including but not limited to the State of New Jersey.

---

[1] Viacom.com, Viacom Company Overview, http://www.viacom.com/brands/pages/nickelodeon.aspx (last visited October 7, 2013).
[2] Google.com, Google Company Overview, http://www.google.com/about/company (last visited October 7, 2013).

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises in part under federal statutes, namely 18 U.S.C. §2710, et seq. (the Video Privacy Protection Act), 18 U.S.C. §2510, et seq. (the Electronic Communications Privacy Act), and 18 U.S.C. § 2701 et seq. (the Stored Communications Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any Defendant.

22. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

23. Venue is proper in this District pursuant to 28 U.S.C. §1391 because a substantial amount of the conduct giving rise to this cause of action occurred in this District and because the United States Judicial Panel on Multidistrict Litigation transferred this case to this District for consolidated pretrial proceedings pursuant to Transfer Order in MDL No. 2443, entered on June 11, 2013.

V. FACTS COMMON TO ALL COUNTS

A. How Do Internet Users Access Websites?

24. In order to access and communicate on the Internet, people employ web-browsers such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

25. Every website is hosted by a computer server, which communicates with an individual's web-browser to display the contents of webpages on the monitor or screen of their individual device.

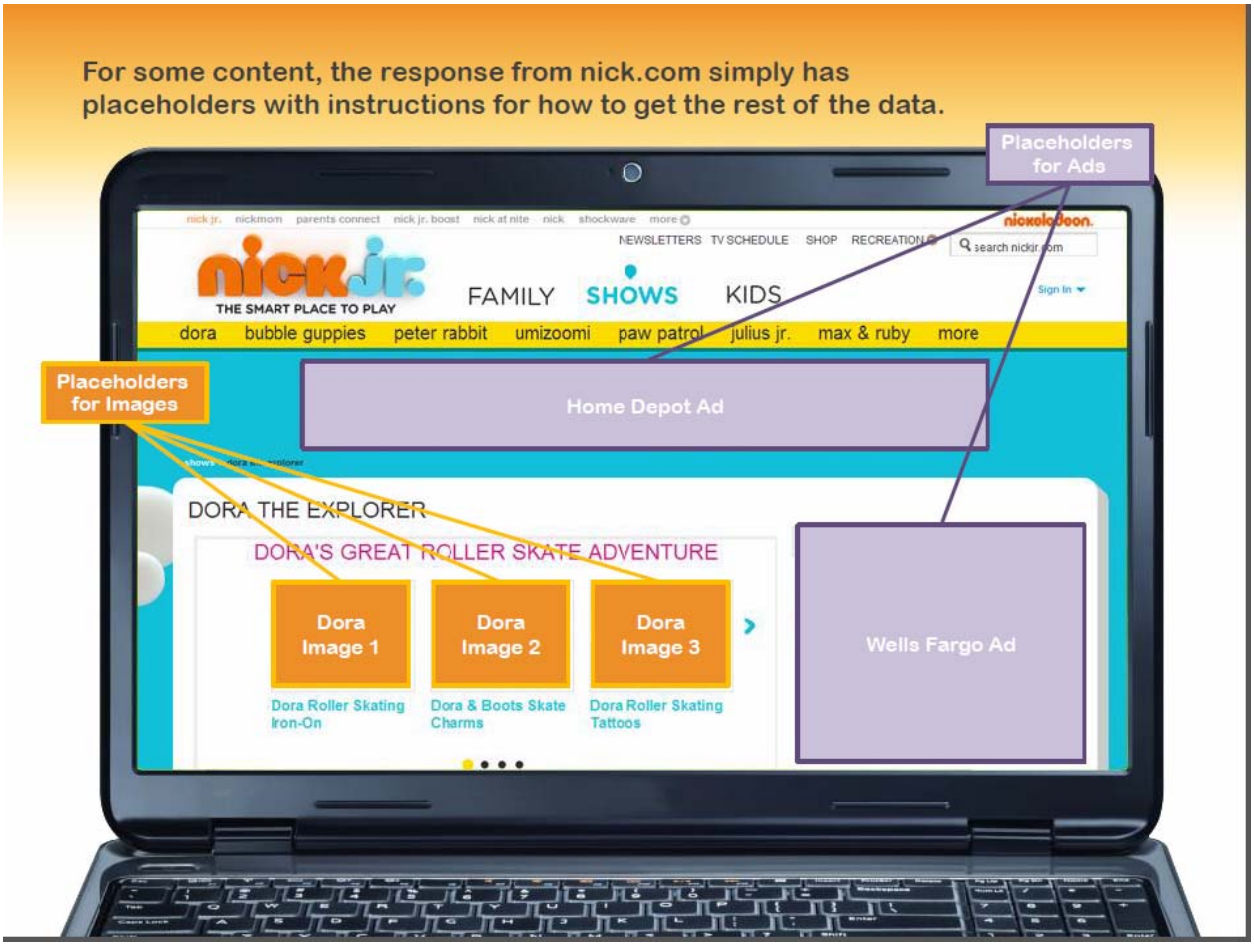
26. The basic command web browsers use to communicate with website servers is

called the "GET" command.

27. For instance, when a child types "www.nick.com" into the navigation bar of his or her web-browser and hits "Enter," the child's web browser sends a "GET" command to the Nick.com host server. The "GET" command instructs the Nick.com host server to send the information contained on Nick.com to the child's browser for display. Graphically, the concept is illustrated as follows:

28. Although a single webpage appears on the child's screen as a complete product, a single webpage is in reality an assembled collage of independent parts. Each different element of a webpage – *i.e.* the text, pictures, advertisements and sign-in box – often exist on distinct servers, which are sometimes operated by separate companies.

29. To display each of these parts of the webpage as one complete product, the host server leaves part of its website blank.



30. Upon receiving a GET command from a child's web browser, the website host server contemporaneously instructs the child's web browser to send other GET commands to other servers responsible for filling in the blank parts of the web page.

31. Those other servers respond by sending information to fill in the blank portions of the webpage.

B. Targeted Internet Advertising: How Does it Work?

32. In the Internet's formative years, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

33. Computer programmers eventually developed technologies commonly referred to as Internet "cookies," which are small text files that web servers can place on a person's computing device when that person's web browser interacts with the website host server.

34. Cookies can perform different functions; and some cookies were eventually designed to track and record an individual's activity on websites across the Internet.

35. In general, cookies are categorized by:

(1) "time" – the length of time they remain on a user's device; and

(2) "party" – describing the relationship (first or third party) between the Internet user and the party who places the cookie:

a. Cookie Classifications by *Time:*

i. "Session cookies" are placed on a person's computing device only for the time period during which the person is navigating the website that placed the cookie. The person's web browser normally deletes session cookies when he or she closes the browser; and

ii. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a "persistent cookie" can record a person's Internet browsing history and Internet communications for years. By virtue of their lifespan, persistent cookies can track a person's communications across the Internet. Persistent cookies are also sometimes called "tracking cookies."

b. Cookie Classifications by *Party*

i. "First-party cookies" are set on a person's device by the website the person intends to visit. For example, Defendant Viacom sets a collection of Nick.com cookies when a child visits Nick.com. First-party cookies can be helpful to the user, server and/or website to assist with security, login

and functionality; and

ii. "Third-party cookies" are set by website servers other than the server the person intends to visit. For example, the same child who visits Nick.com will also have cookies placed on his or her device by third-party web servers, including advertising companies like Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling and targeted advertising.

36. In addition to the information obtained by and stored within third party cookies, third party web servers can be granted access to profile and other data stored within first party cookies.

37. Enterprising online marketers, such as defendants, have developed ways to monetize and profit from these technologies. Specifically, third party persistent "tracking" cookies are used to sell advertising that is customized based upon a particular person's prior Internet activity.

38. Website owners such as Viacom can now sell advertising space on their web pages to companies who desire to display ads to children that are customized based on the child's Internet history.

39. Moreover, many commercial websites with extensive advertising allow third-party companies such as Google to serve advertisements directly from third-party servers rather than through the first party website's server.

40. To accomplish this, the host website leaves part of its webpage blank. Upon receiving a "GET" request from an individual's web browser, the website server will,

unbeknownst to that individual, immediately and contemporaneously re-direct the user's browser to send a "GET" request to the third-party company charged with serving the advertisements for that particular webpage.

41. Some websites contract with multiple third-parties to serve ads such that the website will contemporaneously instruct a user's browser to send multiple "GET" requests to multiple third-party websites.

42. In many cases, the third party receives the re-directed "GET" request and a copy of the user's request to the first-party website before the content of the initial request from the first-party webpage appears on the user's screen.

43. The transmission of such information is contemporaneous to the user's communication with the first-party website.

44. The third-party server then responds by sending the ad to the user's browser – which then displays it on the user's device.

45. In the process of placing advertisements, third-party advertising companies also implant third-party cookies on individuals' computers. They further assign each specific user a unique numeric or alphanumeric identifier that is associated with that specific cookie.

46. The entire process occurs within milliseconds and the web page appears on the individual's web browser as one complete product, without the person ever knowing that multiple GET requests were executed by the browser at the direction of the web site server, and that first party and third party cookies were placed. Indeed, all the person has done is type the name of a single web page into his or her browser. Graphically, the concept is illustrated as follows:

47. Because advertising companies serve advertisements on multiple sites, their cookies also allow them to monitor an individual's communications over every website and webpage on which the advertising company serves ads. And because that cookie is associated with a unique numeric or alphanumeric identifier, the data collected can be utilized to create detailed profiles on specific individuals.

48. By observing the web activities and communications of tens of millions of Internet users, advertising companies, including Defendant Google, build digital dossiers of each individual user and tag each individual user with a unique identification number used to aggregate their web activity. This allows for the placement of "targeted" ads.

C. The Personal Information Defendants Collect: What is Its Value?

49. To the advertiser, targeted ads provided an unprecedented opportunity to reach potential consumers. The value of the information that Defendants take from people who use the Internet is well understood in the e-commerce industry. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[3]

50. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute, Christopher Soghoian, noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[4]

51. In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[5]

---

[3] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

[4] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

[5] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Business and Policymakers – Preliminary FTC Staff Report*, December

52. In general, behaviorally targeted advertisements based on a user's tracked internet activity sell for at least *twice* as much as non-targeted, run-of-network ads.[6]

53. Upon information and belief, most of the Defendants' advertising clients pay on a cost-per-click basis.

54. The Defendants also offer cost-for-impression ads, which charge an advertising client each time the client's ad displays to a user.

55. In general, behaviorally-targeted advertisements produce 670 percent more clicks on ads per impression than run-of-network ads. Behaviorally-targeted ads are also more than twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.[7]

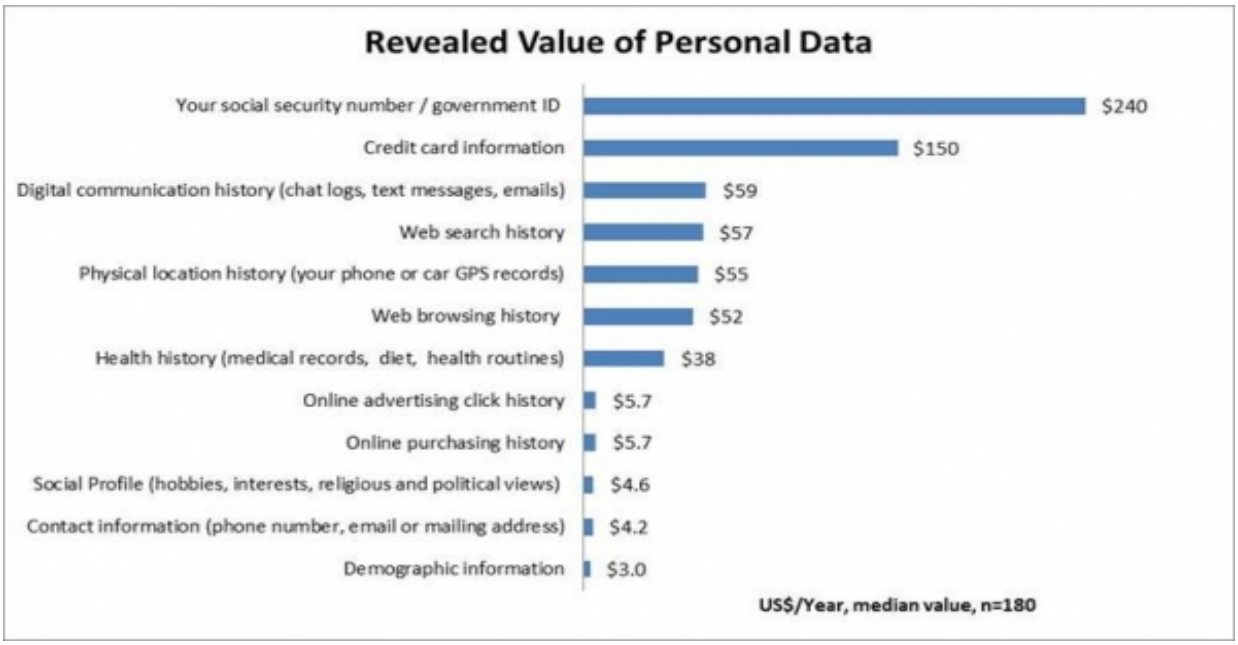
56. The cash value of users' personal information can be quantified. For example, in a recent study authored by Tim Morey, researchers studied the value that 180 Internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. Web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings[8]:

2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37 (last visited October 22, 2013).

[6] NetworkAdvertising.org, *Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads*, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (last visited September 16, 2013).

[7] Howard Beales, *The Value of Behavioral Advertising*, 2010 http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited September 16, 2013).

[8] Tim Morey, *What's Your Personal Data Worth?*, January 18, 2011, http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html (last visited September 16, 2013).



57. In 2012, Defendant Google convened a panel called "Google Screenwise Trends" through which Google paid Internet users to track their online communications through gift cards, with most valued at $5. Though it is unclear whether Google continues to operate Screenwise Trends in the United States,[9] the project remains active in the U.K., where users are paid £15 for staying with Screenwise Trends for 30 days after sign-up and an additional £5 for every 90 days users remain with the panel.[10] Google's Screenwise Trends program demonstrates conclusively that Internet industry participants, including the Defendants, recognize the enormous value in tracking user's Internet communications.

58. Targeting advertisements to children adds *more* value than targeting to adults because children are generally unable to distinguish between content and advertisements. This is

[9] See Screenwisepanel.com, Sign-in Page, https://www.screenwisepanel.com/member/Index.aspx?ReturnUrl=%2fmember, (last visited Sept. 25, 2013) (plaintiffs believe this is the sign-in page for Screenwise Trend users in the United States, indicating the program is still in existence).

[10] See Screenwisetrendspanel.com, Rewards, https://www.screenwisetrendspanel.co.uk/nrg/rewards.php (last visited Sept. 25, 2013).

especially true in the digital realm where children are less likely to identify and counteract the persuasive intent of advertising. This results in children, especially those below the age of 8, accepting advertising information contained in commercials "uncritically . . . [and as] truthful, accurate, and unbiased."[11]

59. An investigation by the Wall Street Journal revealed that "popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults."[12]

D. Internet Tracking: Is it Anonymous?

60. Though industry insiders claim publicly that tracking is anonymous, experts in the field disagree. For instance, in a widely cited blog post for The Center for Internet and Society at Stanford Law School titled "There is No Such Thing as Anonymous Online Tracking," Professor Arvind Narayanan explained:

> In the language of computer science, clickstreams – browsing histories that companies collect – are not anonymous at all; rather, they are pseudonymous. The latter term is not only more technically appropriate, it is much more reflective of the fact that at any point after the data has been collected, the tracking company might try to attach an identity to the pseudonym (unique ID) that your data is labeled with. Thus, identification of a user affects not only future tracking, but also retroactively affects the data that's already been collected. Identification needs to happen only once, ever, per user.

---

[11] Report of the APA Task Force on Advertising and Children at 8 available at http://www.apa.org/pi/families/resources/advertising-children.pdf; see also, Louis J. Moses, *Research on Child Development: Implications for How Children Understand and Cope with Digital Marketing*, MEMO PREPARED FOR THE SECOND NPLAN/BMSG MEETING ON DIGITAL MEDIA AND MARKETING TO CHILDREN, June 29-30, 2009, http://digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (last visited October 22, 2013).

[12] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, THE WALL STREET JOURNAL, September 17, 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html (last visited September 16, 2013).

> Will tracking companies actually take steps to identify or deanonymize users? It's hard to tell, but there are hints that this is already happening: for example, many companies claim to be able to link online and offline activity, which is impossible without identity.[13]

61. Moreover, any company employing re-identification algorithms can precisely identify a particular consumer:

> It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.
>
> The versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning. While some attributes may be uniquely identifying on their own, any attribute can be identifying in combination with others.[14]

62. The Federal Trade Commission has recognized the impossibility of keeping data derived from cookies and other tracking technologies anonymous, stating that industry, scholars, and privacy advocates have acknowledged that the traditional distinction between the two categories of data [personally identifiable information and anonymous information] has eroded and is losing its relevance.[15]

63. For example, in 2006, AOL released a list of 20 million web search queries connected to "anonymous" ID numbers, including one for user No. 4417749. Researchers were

---

[13] Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, The Center for Internet and Society Blog, July 28, 2011, http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking (last visited September 16, 2013).

[14] Arvind Narayanan, *Privacy and Security Myths of Fallacies of "Personally Identifiable Information*," Communications of the ACM, June 2010, http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf (last visited September 16, 2013).

[15] FTC.gov, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited September 16, 2013).

quickly able to identify specific persons with the so-called anonymous ID numbers. As explained by the New York Times:

> The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.
> . . . .
> [T]he detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines – and how risky it can be for companies like AOL, Google, and Yahoo to compile such data." [16]

64. Another technological innovation is the use of "browser fingerprinting," which allows websites to "gather and combine information about a consumer's web browser configuration – including the type of operating system used and installed browser plug-ins and fonts – to uniquely identify and track the consumer.[17]

65. Another recent innovation, as Prof. Narayanan predicted, is for companies to connect online dossiers with offline activity. As described by one industry insider:

> With every click of the mouse, every touch of the screen, and every add-to-cart, we are like Hansel and Gretel, leaving crumbs of information everywhere. With or without willingly knowing, we drop our places of residence, our relationship status, our circle of friends and even financial information. Ever wonder how sites like Amazon can suggest a new book you might like, or iTunes can match you up with an artist and even how Facebook can suggest a friend?
>
> Most tools use first-party cookies to identify users to the site on their initial and future visits based upon the settings for that particular solution. The information generated by the cookie is transmitted across the web and used to segment visitors' use of the website and to compile statistical reports on website activity. This leaves analytic vendors – companies like Adobe, Google, and IBM – *the ability to combine online with offline data*, creating detailed profiles and serving

[16] Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times., Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=print (last visited September 16, 2013).
[17] FTC.gov, *supra* note 15 at 36.

targeted ads based on users' behavior.[18]

66. On information and belief, the Defendants in this case are able to link online and offline activity and identify specific users, including the plaintiffs and children that form the putative class.

67. The Defendants, in fact, have marketed their ability to target individual users by connecting data obtained from first-party and third-party cookies.

68. Specifically, Defendant Viacom holds itself out to advertisers as being able to target users with "pinpoint accuracy" to reach "specific audiences on every digital platform" by "connecting the dots between first and third-party data to get at user attributes including interests, behaviors, demo, geolocation, and more."[19] Viacom does this through its "Surround Sound" service powered through Adobe's Audience Manager product. Viacom Vice President for Digital Products, Josh Cogswell, has said publicly the product can be used to target "kids" and, regarding Viacom's audience, "We know who you are across our sites."

69. Moreover, Defendant Google's website informs potential ad buyers that it can identify web users with Google's DoubleClick.net cookies:

> For itself, Google identifies users with cookies that belong to the doubleclick.net domain under which Google serves ads. For buyers, Google identifies users using a buyer-specific Google User ID which is an encrypted version of the doubleclick.net cookie, derived from but not equal to that cookie.[20]

---

[18] Tiffany Zimmerman, *Data Crumbs*, June 19, 2012, http://www.stratigent.com/community/analytics-insights-blog/data-crumbs (last visited September 16, 2013) (emphasis added).

[19] Viacom.com, Serving Advertisers in Surround Sound, March 26, 2012, http://blog.viacom.com/2012/03/serving-advertisers-in-surround-sound-2/ (last visited September 16, 2013) ("Kids" admission at 5:17 of video; "We know who you are across our sites," at 6:25 of video).

[20] Google.com, Google Developer Cookie Guide, https://developers.google.com/adexchange/rtb/cookie-guide (last visited September 16, 2013).

70. In addition, Defendant Google announced a new service in December 2012 called the DoubleClick Search API Conversion Service that will allow advertisers to integrate offline activity with online tracking.[21]

71. Viacom and Google use the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage and the content of the their web communications, including, but not limited to, videos requested and obtained.

E. Viacom and the Third Party Tracker Defendants: How Do They Track Children's Internet Use?

72. Immediately upon the Plaintiffs' first communication with the Viacom children's websites, Defendant Viacom automatically placed its own first party cookies on the computing devices of the Plaintiffs.

73. Additionally, immediately upon the Plaintiffs' first communication with the Viacom children's websites, Viacom knowingly permitted Defendant Google to place its own third-party cookies on the computing devices of the Plaintiffs, or alternatively, to access the information stored within those cookies if the cookies already existed on the user's device by virtue of Plaintiffs having visited another website affiliated with Google.

74. Viacom allowed Google to place and/or access cookies from its doubleclick.net domain.

75. Upon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first party cookies.

76. The placement and/or access of these cookies occurred before either the Plaintiffs or their legal guardians had the opportunity to consent to their placement and/or access to the

[21] Google.com, DS API Interface – Conversion Service Overview, https://support.google.com/ds/answer/2604604?hl=en (last visited September 16, 2013).

Plaintiffs' Internet communications.

77. Google's third-party cookies tracked, among other things, the URLs (Uniform Resource Locators) visited by the Plaintiffs, the Plaintiffs' respective IP addresses and each Plaintiff's browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with Viacom's children's websites.

78. A URL is composed of several different parts.[22] For example, consider the following URL: http://www.nick.com/shows/penguins-of-madagascar/:

a. **http://**: This is the protocol identified by the web browser to the web server which sets the basic language of the interaction between browser and server. The back-slashes indicate that the browser is attempting to make contact with the server;

b. **www.nick.com**: This is the name that identifies the website and corresponding web server, with which the Internet user has initiated a communication;

c. **/shows/**: This part of the URL indicates a folder on the web server, a part of which the Internet user has requested;

d. **/penguins-of-madagascar/**: This is the name of the precise file requested; and

e. **/shows/penguins-of-madagascar/**: This combination of the folder and exact file name is called the "file path".

[22] Microsoft.com, URL Path Length Restrictions (Sharepoint Server 2010), Aug. 5, 2010, http://technet.microsoft.com/en-us/library/ff919564(v=office.14).aspx, (last visited October 21, 2013).

79. Graphically, the concept is illustrated as follows:

80. The URLs visited by plaintiffs and putative class members contain, among other things, substantive content. For instance, in the foregoing example the URL file path contains the substance, purport and meaning of the user's communication with Nick.com, namely, it identifies the exact title of the video the user has requested and received.

81. On its web sites, Viacom further disclosed to Google at least the following about each Plaintiff who was a registered user of Viacom's children's websites: (1) the child's username; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system;

(8) the child's screen resolution; (9) the child's browser version; and (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites.

82. Google's third party cookies assigned to each Plaintiff a unique numeric or alphanumeric identifier that then became connected to (1) the child's username; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser setting; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; and (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites.

83. Upon information and belief, with the information they obtain, Defendants Viacom and Google were able to identify specific individuals and connect online communications and data, including video viewing histories of the Plaintiffs, to offline communications and data.

84. Viacom and Google used the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage, including videos requested and obtained.

F. Viacom and the Third Party Tracking Defendants: What Did They Know About the Gender and Age of Viacom Users?

85. Upon arriving on the Viacom Children's websites, Viacom encouraged its users to register and establish profiles for those websites.

86. During the registration process, Viacom obtained the birthdate and gender of its users.

87. Viacom gave its users an internal code name based upon their answers to the

gender and birth date questions.

88. For instance, Viacom gave 6 year-old males the code name "Dil", and 12 year-old males the code name "Lou".

89. Viacom calls this coding mechanism the "rugrat" code.

90. When a child registered for an account, the child would also create a unique profile name that was tied to that child's profile page.

91. Viacom associated each profile name with a first party identification cookie that had its own unique numeric or alphanumeric identifier.

92. Viacom allowed Google to access each child's profile name.

93. Viacom also provided Google with the code name for the child's specific gender and age.

94. Google was then able to associate the child's age, gender, and other information with its own DoubleClick cookie's unique numeric or alphanumeric identifier so that each time the DoubleClick cookie was accessed, Google would know the specific child they were tracking.

G. How Did Defendants Viacom and Google Share the Video Viewing Histories of Minor Children?

95. The Viacom children's websites offer children the ability to view and/or interact with video materials.

96. When a child viewed a video, or played a video game on a Viacom site, an online record of the activity was made.

97. Viacom provided Google with the online records disclosing its users' video viewing activities.

98. For instance, the following video viewing activity of a Nick.com user was provided to Google and stored within Google's doubleclick.net domain cookies:

> http://ad.doubleclick.net/adi/nick.nol/atf_i_s/club/clubhouses/***penguins_of_madagascar*** [23] ;sec0=clbu;sec1=clubhouses;sec2=penguins_of_madagascar;cat=2;***rugrat=Dil*** [24] ;lcategory=pom_teaser;show=pom_teaser;gametype=clubhouses;demo=D;site=nick;lcategory=nick;u= ***. . . [the user's unique third party cookie alphanumeric identifier appears at the end of the string]***)

99. The online record Viacom provided to Google included the code name that specified the child's gender and age, which in the foregoing example is rugrat=Dil, denominating a male user, age 6.

100. Because Google also received an online record when a child logged in or visited his or her profile page, Google could use its unique numeric or alphanumeric identifier to associate the video materials watched by a specific child with the profile name and profile page of that specific child.

101. From this data, Google was able to compile a history of any particular child's video viewing activity.

102. At no point did Viacom or Google seek or receive the informed, written consent of any Plaintiff or their parent to disclose the video materials requested and obtained by the Plaintiffs from Viacom's children's websites to a third-party at the time such disclosure was sought and effectuated.

VI. CLASS ACTION ALLEGATIONS

103. This putative class action is brought pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3). The Plaintiffs bring this action on behalf of themselves and all similarly situated minor children under the age of 13 as representatives of a class and a subclass defined as follows:

[23] *Penguins of Madagascar* is the name of the video requested by this user.
[24] "Dil" is the code name Viacom gives to male users, age 6.

> **U.S. Resident Class**: All children under the age of 13 in the United States who visited the websites Nick.com, NickJr.com, and/or NeoPets.com, and had Internet cookies that tracked their Internet communications placed on their computing devices by Viacom and Google.
>
> **Video Subclass**: All children under the age of 13 in the United States who were registered users of Nick.com, NickJr.com, and/or NeoPets.com, who engaged with one or more video materials on such site(s), and who had their video viewing histories knowingly disclosed by Viacom to Google.

104. Each Plaintiff meets the requirements of both the U.S. Resident Class and Video Subclass.

105. The particular members of the proposed Class and Subclass are capable of being described without managerial or administrative difficulties. The members of the Class and Subclass are readily identifiable from the information and records in the possession or control of the Defendants.

106. The members of the Class and Subclass are so numerous that individual joinder of all members is impractical. This allegation is based upon information and belief that Defendants intercepted the video-viewing histories and Internet communications of millions of Nick.com, NickJr.com and NeoPets.com users.

107. There are questions of law and fact common to the Class and Subclass that predominate over any questions affecting only individual members of the Class or Subclass, and, in fact, the wrongs suffered and remedies sought by the Plaintiffs and other members of the Class and Subclass are premised upon an unlawful scheme participated in by each of the Defendants. The principal common issues include, but are not limited to, the following:

a. Whether Viacom constitutes a video tape service provider as defined in the Video Privacy Protection Act;

b. Whether the Plaintiffs constitute consumers as defined in the Video Privacy Protection Act;

c. The nature and extent to which video materials requested and obtained by Viacom website users were disclosed in violation of the Video Privacy Protection Act;

d. Whether the Defendants "intercepted" the electronic communications of members of the Class in violation of the Electronic Communications Privacy Act;

e. Whether the Defendants utilized "devices" to intercept the online communications of the class;

f. Whether the Defendants intercepted "content" as described in the Electronic Communications Privacy Act;

g. Whether the Defendants intercepted the online communications of the Plaintiffs for a criminal or tortious purpose;

h. Whether the actions taken by the Defendants violate the Stored Communications Act;

i. Whether the Defendants accessed a "facility" as described in the Stored Communications Act;

j. Whether the Defendants accessed a facility without authorization as described in the Stored Communications Act;

k. Whether the actions taken by the Defendants violate the California Invasion of Privacy Act;

l. Whether the actions taken by the Defendants violate the New Jersey Computer Related Offenses Act;

m. Whether or not Viacom should be enjoined from further disclosing information

about the video materials its minor children users watch on its sites, and whether Google should be enjoined from further accessing such information without the proper consent of Plaintiffs;

n. Whether or not the Defendants should be enjoined from further intercepting any electronic communications without the proper consent of the Plaintiffs;

o. Whether the Defendants intruded upon the Plaintiffs' seclusion;

p. Whether the Plaintiffs are entitled to recover profits gained at their expense by the Defendants under a claim for unjust enrichment;

q. The nature and extent of all statutory penalties or damages for which the Defendants are liable to the Class and Subclass members; and

r. Whether punitive damages are appropriate.

108. The common issues predominate over any individualized issues such that the putative class is sufficient cohesive to warrant adjudication by representation.

109. The Plaintiffs' claims are typical of those of the members of the Class and Subclass and are based on the same legal and factual theories.

110. Class treatment is superior in that the fairness and efficiency of class procedure in this action significantly outweighs any alternative methods of adjudication. In the absence of class treatment, duplicative evidence of Defendant's alleged violations would have to be provided in thousands of individual lawsuits. Moreover, class certification would further the policy underlying Rule 23 by aggregating class members possessing relatively small individual claims, thus overcoming the problem that small recoveries do not incentivize plaintiffs to sue individually.

111. The Plaintiffs, by and through their Next Friends, will fairly and adequately

represent and protect the interests of the members of the Class. The Plaintiffs have suffered injury in their own capacity from the practices complained of and are ready, willing, and able to serve as Class representatives. Moreover, Plaintiffs' counsel is experienced in handling class actions and actions involving unlawful commercial practices, including such unlawful practices on the Internet. Neither the Plaintiffs nor their counsel has any interest that might cause them not to vigorously pursue this action. The Plaintiffs' interests coincide with, and are not antagonistic to, those of the Class members they seek to represent.

112. Certification of a class under Federal Rule of Civil Procedure 23(b)(2) is appropriate because the Defendants have acted on grounds that apply generally to the Class such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

113. Certification of a class under Federal Rule of Civil Procedure 23(b)(3) is appropriate in that the Plaintiffs and the Class Members seek monetary damages, common questions predominate over any individual questions, and a plaintiff class action is superior for the fair and efficient adjudication of this controversy. A plaintiff class action will cause an orderly and expeditious administration of Class members' claims and economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured. Moreover, the individual members of the Class are likely to be unaware of their rights and not in a position (either financially or through experience) to commence individual litigation against these Defendants.

114. Alternatively, certification of a plaintiff class under Federal Rule of Civil Procedure 23(b)(1) is appropriate in that inconsistent or varying adjudications with respect to individual members of the Class would establish incompatible standards of conduct for the Defendants or adjudications with respect to individual members of the Class as a practical matter

would be dispositive of the interests of the other members not parties to the adjudication or would substantially impair or impede their ability to protect their interests.

COUNT I – VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT

Children's Video Subclass v. All Defendants

115. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

116. Online video streaming is quickly replacing the traditional brick and mortar video rental store.

117. The Video Privacy Protection Act, 18 U.S.C. § 2710, (hereinafter "VPPA"), makes it illegal for a video tape service provider to knowingly disclose personally identifiable information concerning any consumer of such provider to a third-party without informed written consent by the consumer given at the time such disclosure is sought.

a. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials."

b. As defined in 18 U.S.C. § 2710(a)(3), "personally identifiable information" is that which "identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

c. As defined in U.S.C. § 2710(a)(1) a "consumer" means "any renter, purchaser or subscriber of goods or services from a video tape service provider."

118. As specified in 18 U.S.C. § 2710(b)(2)(B) at the time this action was filed, valid consent under the VPPA is the "informed, written consent of the consumer given at the time the

disclosure is sought."[25]

119. The Video Privacy Protection Act of 1988 was passed for the explicit purpose of protecting the privacy of specific individuals' video requests and viewing histories.

120. At the time of its passage, Congress was well aware of the impact of ever-changing computer technology. Upon the VPPA's introduction, the late Senator Paul Simon noted:

> There is no denying that the computer age has revolutionized the world. Over the past 20 years we have seen remarkable changes in the way each of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. *The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before.* Every day Americans are forced to provide to businesses and others 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) (emphasis added).

121. Senator Patrick Leahy also remarked at the time that new privacy protections were needed:

[25] After years of lobbying by online video service providers, Congress amended the "consent" portion of the VPPA. This action was brought under this previous definition of "consent." The new definition, also found in 18 U.S.C. § 2710 (b)(2)(B) provides that consent must be "informed, written consent (including through an electronic means using the Internet of the consumer that – (i) is in a form distinct and separate from an form setting forth other legal or financial obligations of the consumer; (ii) at the election of the consumer—(I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election."

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

S. Rep. No. 100-599 at 5-6 (1988).

122. Sen. Leahy later explained:

> It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not anybody else's business, whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business."[26]

123. The sponsor of Act, Rep. Al McCandless, also explained:

> There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of intellectual thought. The whole process of intellectual growth is one of privacy – of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

S. Rep. No. 100-599 at 7.

124. Online video service providers were well-aware of the restrictions imposed by the VPPA. For instance, in 2012, online video service provider Netflix lobbied for legislation to amend the Act to no longer require consent every time it sought to disclose a video requested or viewed by a customer.

[26] GPO.gov, House Report 112-312, December 2, 2011, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt312/html/CRPT-112hrp312.htm (last visited September 16, 2013.

125. As stated clearly in the legislative history to the VPPA amendments of 2012:

> Since 1988, Federal law has authorized video tape service providers to share customer information with the 'informed, written consent of the consumer at the time the disclosure is sought.' This consent must be obtained each time the provider wishes to disclose.

House Report 112-312 at 4. (2012).

126. Viacom is engaged in the business of the delivery of pre-recorded video cassette tapes or similar audio visual materials as defined by the VPPA in that:

a. The home page of Nick.com advertises it as the place to watch "2000+ FREE ONLINE VIDEOS and "play "1000+ FREE ONLINE GAMES." The homepage prominently features a rotating section enticing users to click and watch various videos with action buttons that say "Watch now," "Check it out," or, in the case of games, "Play Now." In addition, two of the first three links in the top bar on the homepage refer to audio-visual materials. *See* Nick.com (last visited September 24, 2013).

b. The home page of NickJr.com advertises it as the place to watch Dora the Explorer, Bubble Guppies, UmiZoomi, and dozens of other children's shows. It also provides users the ability to play online video games. Immediately upon visiting NickJr.com, the page loads videos that play in the upper right hand portion of the home-page.

c. The home page of NeoPets.com advertises it as the place to play dozens of video games, which are similar audio-visual materials.

127. Plaintiffs and members of the putative video sub-class are "consumers' under the VPPA in that they are registered users of the Viacom children's websites and, therefore, constitute subscribers to the video services Viacom provides on its websites.

128. Viacom violated the VPPA by knowingly disclosing to Google the Plaintiffs' personally identifiable information through the specific video materials and services requested and obtained from Viacom by the Plaintiffs without the Plaintiffs' written consent.

129. Google violated the VPPA by knowingly obtaining Plaintiffs' personally identifiable information in the form of the specific video materials and services requested and obtained by Plaintiffs from Viacom.

130. Defendant Google knowingly accepted the Plaintiffs' personally identifiable information regarding video materials and services through its use of the doubleclick.net cookies and other computer technologies.

131. On information and belief, Google further violated the VPPA by failing to destroy plaintiffs' personally identifiable information as provided in 18 U.S.C. § 2710 (e).

132. As a result of the above violations and pursuant to 18 U.S.C. § 2710, the Defendants are liable to the Plaintiffs and the Class for "liquidated damages of not less than $2,500 per plaintiff; reasonable attorney's fees and other litigation costs; injunctive and declaratory relief; and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future."

COUNT II – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

U.S. Resident Children v. All Defendants

133. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

134. Enacted in 1986, the Electronic Communications Privacy Act ("ECPA") amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. The ECPA prohibits the unauthorized interception of the contents of electronic transmissions such as those made by Plaintiffs in this

case.

135. Representative Kastenmeier discussed the scope the ECPA amendments were designed to reach:

> . . . [L]egislation which protects electronic communications from interceptions…should be comprehensive, and *not limited to particular types or techniques of communicating* . . . . Any attempt to . . . protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years….what is being protected is *the sanctity and privacy of the communication.* We *should not attempt to discriminate for or against certain methods of communication* . . . .[27]

136. Moreover, Senator Leahy discussed the purpose of the ECPA:

> Today Americans have at their fingertips a broad array of telecommunications and computer technology, including . . . *computer-to-computer links* . . . . When title III was written 18 years ago, Congress could barely contemplate forms of telecommunications and computer technology we are starting to take for granted today . . . . Senate bill 2575 . . . is designed to . . . provide a reasonable level of Federal privacy protection to these new forms of communication.[28]

137. As described herein, Google intentionally intercepted the contents of electronic communications of minor children under the age of 13 who visited Nick.com, NickJr.com, and NeoPets.com through Google's use of devices that tracked and recorded the Plaintiffs' web communications, including but not limited to their Internet browsing histories and without consent.

138. Google's DoubleClick.net cookies tracked at least the following information regarding each individual Plaintiff: (1) unique IP address; (2) browser setting; (3) unique device identifier; (4) operating system; (5) screen resolution; (6) browser version; (7) and web

[27] 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Rep. Kastenmeier) (emphasis added).
[28] 132 Cong. Rec. S14441-04 (1986) 1986 WL 786307 (comments from Sen. Leahy) (emphasis added).

communications, including but not limited to detailed and unique URL requests (which included video materials requested and obtained from Viacom's children's websites).

139. The specific Uniform Resource Locators the Plaintiffs typed into and sent through their web browsers are "contents" within the meaning of the ECPA because they include "any information concerning the substance, purport, or meaning of that communication" as defined in 18 U.S.C. § 2510 (8).

140. Specifically, URLs that expose the "file path" contain content under the ECPA. As an example, the URL http://www.nick.com/shows/penguins-of-madagascar/ is content because it contains "information concerning the substance, purport, or meaning of that communication," namely, it identifies the exact title of the video shown on the communication requested and received by the Internet user from Viacom.

141. If an individual called Blockbuster Video to request that Blockbuster mail the video "Penguins of Madagascar" to that individual, and if a third party intercepted the substance of that call, the third party would have intercepted "contents" because it would have received information concerning the substance, purport, or meaning of the individual's communication with Blockbuster, namely, the request for a specific video.

142. The only difference in this case is that the plaintiffs' communications with Viacom in requesting certain videos were executed with a keyboard. Google, thus, intercepted the "contents" of the plaintiffs' requests to Viacom for specific videos; and, as those requests contain the substance, purport and meaning of plaintiffs' communications with Viacom, namely, the request for a specific video, such information constitutes content as defined in the ECPA.

143. Congress also intended for URLs to constitute "content" under the ECPA. In modifying the Pen Register Act through the Patriot Act, the House Committee Report states:

> This section updates the language of the statute to clarify that the pen/register authority applies to modern communication technologies…Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain any non-content information—"dialing, routing, addressing, and signaling information"—utilized in the process of transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979).
>
> Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than "dialing, routing, addressing, and signaling" information, *such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.*[29]

144. Google's tracking and interceptions began immediately upon the Plaintiffs' first communications with Defendant Viacom's children's websites and before any consent could be obtained from the Plaintiffs' and Class Members' guardians.

145. Google's cookies tracked and recorded the content of the web communications of the Plaintiffs and class members contemporaneous to, and, in some cases, before the Plaintiffs' communications with other websites were consummated such that the tracking and recording was contemporaneous with the Plaintiffs' communications and while the communications were in transit.

146. After Plaintiffs registered with the Viacom site, Google also accessed their individual username, gender, and birthdate.

147. Defendant Google's doubleclick.net "id", cookies:

[29] H.R. Rep. 107-236(I) at 53-54 (emphasis added).

a. Were placed on Plaintiffs' computing devices before each Plaintiff created an account or logged-in to the respective Viacom children's websites;

b. Remained on the Plaintiffs' computing devices even after individual users who were minor children under the age of 13 had created an account or logged-in and informed Viacom that they were minor children under the age of 13; and

c. Are capable of determining each individual user's response to Viacom's "birthdate" question in the form which was necessary to create a user account and collects information about the user's age via computer code.

148. The transmission of data between the Plaintiffs' computing devices and Viacom's children's websites and other non-Viacom websites hosted by servers are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

149. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5).

a. Each individual cookie that Google used to track the Plaintiffs' communications;

b. The Plaintiffs' browsers which Google used to place and extract data from each Defendant's individual cookies;

c. The Plaintiffs' computing devices;

d. Each Defendant's web server; and/or

e. The plan Google carried out to effectuate its purpose of tracking the electronic communications of minor children.

150. The Plaintiffs, minor children under the age of 13, did not, and as a matter of law could not have, consented to the tracking of their web usage and communications.

151. The Plaintiffs' legal guardians did not consent to the tracking of Plaintiffs' web usage and communications.

152. Viacom, as a matter of law, could not have consented to the tracking of the web usage and communications of minor children under the age of 13 using their websites without the consent of their guardians.

153. The Defendants' actions were done for the tortious purpose of intruding upon the Plaintiffs' seclusion as set forth in this Complaint.

154. The Defendants' actions were done for criminal purposes in violation of numerous federal and state statutes, including, but not limited to 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act.

155. Upon information and belief, in addition to intercepting the Plaintiffs' communications with the Viacom children's websites, Google used the cookies to track the Plaintiffs' communications with other websites on which Google places advertisements and related tracking cookies despite Google's knowledge that the Plaintiffs were minor children and without the consent of the Plaintiffs, their guardians, or the other websites with which the Plaintiffs were communicating.

156. Viacom procured Google to intercept the content of Plaintiffs' Internet communications with other websites.

157. Upon information and belief, Viacom profited from Google's unauthorized tracking of the Plaintiffs' Internet communications with other websites as such information assisted in the sale of targeted advertisements to children on the Viacom sites.

158. Viacom knew or had reason to know that Google intentionally intercepted the content of the Internet communications of the Plaintiffs on non-Viacom websites with tracking cookies deposited and/or accessed on Viacom's websites despite Google's knowledge that the

Plaintiffs were minor children and that it did not have either the Plaintiffs' or their guardians' consent to intercept their Internet communications.

159. As a direct and proximate cause of such unlawful conduct, the Defendants violated the ECPA in that they:

a. Intentionally intercepted or procured another person to intercept the contents of wire and/or electronic communications of the Plaintiffs;

b. Upon belief predicated upon further discovery, intentionally disclosed to another person the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and

c. Upon belief predicated upon further discovery, intentionally used or endeavored to use the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a).

160. As a result of the above violations, and pursuant to 18 U.S.C. § 2520, the Defendants are liable to the Plaintiffs and the Class in the sum of statutory damages consisting of the greater of $100 for each day each of the class members' data was wrongfully obtained or $10,000 per violation, whichever is greater; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future, and reasonable attorney's fees and other litigation costs.

COUNT III – THE STORED COMMUNICATIONS ACT

U.S. Resident Children v. Google

161. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

162. The Stored Communications Act (hereinafter "SCA") provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," or any person "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

163. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

164. The SCA defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

165. Defendants intentionally accessed without authorization or intentionally exceeded authorization to access facilities through which an electronic communications services was provided when they used the instrumentalities described in this Complaint to access the Plaintiffs' web-browsers and computing devices for purposes of tracking the Plaintiffs' Internet communications.

166. The web browsers utilized by the Plaintiffs on their computing devices provide electronic communications services to the Plaintiffs because they "provide to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

167. The Internet Service Providers to which the Plaintiffs use or subscribe to provide electronic communication services to the Plaintiffs because they "provide to users thereof the

ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

168. Neither the Plaintiffs' browsers nor the Internet Service Providers authorized the extent of the Defendants' access to the Plaintiffs' computing devices.

169. The Plaintiffs' respective web browsers store cookie and other information in browser-managed files on the Plaintiffs' computing devices. These browsers are also facilities under the SCA because they comprise the software necessary for and "through which (the) electronic communications service is provided."

170. Google intentionally accessed Plaintiffs' web browsers without authorization when Google accessed Plaintiffs' browsers immediately upon the Plaintiffs' visiting Viacom's children's websites and after sign-up without obtaining the consent of the Plaintiffs or their guardians.

171. The Plaintiffs' computing devices are facilities under the SCA because they comprise the hardware necessary for and "through which (the) electronic communications service is provided."

172. The cookies in the browser-managed files that Plaintiffs' web browsers store are updated regularly to record users' browsing activities and communications as they happen. For that reason, when Google accesses these facilities to acquire Plaintiffs' electronic communications, it acquires profile information and related just-transmitted electronic communications out of random access memory ("RAM"). Google acquires the profile information and related electronic communications out of electronic storage, incidental to the transmission thereof.

173. Upon information and belief, the acquisition of electronic communications from the Plaintiffs' web browsers and computing devices included the contents of communications the

Plaintiffs had with non-Viacom websites that are not affiliated with Google.

174. Plaintiffs and Class Members were harmed by Defendant's violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendants attributable to the violations or statutory minimum damages of $1,000 per person, punitive damages, costs, and reasonable attorney's fees.

COUNT IV – THE CALIFORNIA INVASION OF PRIVACY ACT

U.S. Resident Children v. All Defendants

175. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

176. California Penal Code § 631(a) provides, in pertinent part:

> Any person who . . . willfully and without the consent of *all* parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

(emphasis added).

177. The Defendants' tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications, including web-browsing and video-viewing histories, was done without authorization or consent of either the Plaintiffs and Class Members or their guardians.

178. Google's corporate headquarters are located in California.

179. On information and belief, a substantial portion of the putative class and plaintiff L.G. reside in the State of California and accessed the Viacom Children's websites from

computing devices in the state of California.

180. Upon information and belief, Google directed and used the tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications in the state of California.

181. As a result of Google's actions in California, every act of tracking and every interception of the Plaintiffs' and Class Members' personal information and Internet communications took place, in part, in California, regardless of the location of each individual Plaintiff and Class Member.

182. Plaintiffs and Class Members did not consent to any of the third-party tracker Defendants' actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

183. Plaintiffs and Class Members, as a matter of law, could not have consented to Google's actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

184. Viacom aided, conspired with, and permitted Google to violate California Penal Code § 631(a) when Viacom permitted, acquiesced to, facilitated, and participated in the activity alleged herein by knowingly serving as the conduit through which Google placed its devices in positions to intercept the content of Plaintiffs' Internet communications. Viacom then profited from Google's interceptions through the sale of targeted advertisements to Plaintiffs on Viacom's children's websites.

185. Plaintiffs and Class Members have suffered loss by reason of these violations including, but not limited to, violation of their rights of privacy and loss of value in their Personally Identifiable Information.

186. Unless restrained and enjoined, the Defendants will continue to commit such acts.

187. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and the Class Members have been injured by the violations of Cal. Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, whichever is greater, as well as injunctive relief.

COUNT V – NEW JERSEY COMPUTER RELATED OFFENSES ACT

U.S. Resident Children v. All Defendants

188. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

189. N.J.S.A. 2A:38A-3 states that a person or enterprise is liable for:

a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;

c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;

d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or

e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

190. Defendants did purposefully, knowingly and/or recklessly, without Plaintiffs',

Class Members' or their respective guardians' authorization, access, attempt to access, tamper with, alter, damage, take, destroy, obtain and/or intercept Plaintiffs' and Class Members' computer, computer software, data, database, computer program, computer system, computer equipment and/or computer network in violation of N.J.S.A. 2A:38A-1 et seq.

191. Many of the computers that were accessed, the terminal used in the accessing, and/or the actual damages took place in New Jersey.

192. Plaintiffs C.A.F., C.T.F., M.P. and T.P. all reside in the State of New Jersey and accessed the Viacom Children's sites from computing devices within the State of New Jersey.

193. Pursuant to N.J.S.A. 2A:38A-1 et seq., Plaintiffs and the Class Members have been injured by the violations of N.J.S.A. 2A:38A-1 et seq., and each seek damages for compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation, as well as injunctive relief.

COUNT VI – INTRUSION UPON SECLUSION

U.S. Resident Children v. All Defendants

194. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

195. In carrying out the scheme to track the Plaintiffs' Internet communications as described herein without the consent of the Plaintiffs or their legal guardians, the Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion in that the Defendants took information from the privacy of the Plaintiffs' homes.

196. The Plaintiffs, minor children, did not, and by law could not, consent to the Defendants' intrusion.

197. The Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion would be highly offensive to a reasonable person.

COUNT VII – UNJUST ENRICHMENT

U.S. Resident Children v. All Defendants

198. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

199. Plaintiffs conferred a benefit on Defendants without Plaintiffs' consent or the consent of their parents or guardians, namely, access to wire or electronic communications and Plaintiffs' personal information over the Internet.

200. Upon information and belief, Defendants realized such benefits either through sales to third-parties or greater knowledge of its users' behavior without their consent.

201. Acceptance and retention of such benefit without Plaintiffs' consent is unjust and inequitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class Members and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class Members against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

E. Permanently restrain Defendants, and their officers, agents, servants, employees, and attorneys, from tracking their users without consent or otherwise violating their policies with

users;

F. Award Plaintiffs and the Class Members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

G. Order that Defendants delete the data they collected about users through the unlawful means described above; and

H. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 23, 2013

Respectfully submitted,

EICHEN CRUTCHLOW ZASLOW & McELROY, LLP
Barry R. Eichen, Esq.
Evan J. Rosenberg, Esq.
40 Ethel Road
Edison, NJ 08817
Tel.: (732) 777-0100
Fax: (732) 248-8273
beichen@njadvocates.com
erosenberg@njadvocates.com

and

/s/ James P. Frickleton
BARTIMUS, FRICKLETON, ROBERTSON & GORNY P.C.
James P. Frickleton, Esq.
Edward D. Robertson III, Esq.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: (913) 266 2300
Fax: (913) 266 2366
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson Jr. Esq.
Mary D. Winter Esq.
715 Swifts Highway
Jefferson City, MO 65109
Tel: (573) 659 4454
Fax: (573) 659 4460
chiprob@earthlink.net
marywinter@earthlink.net

Attorneys for Plaintiffs