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
This Document Relates to: **All Actions**	**SECOND CONSOLIDATED CLASS ACTION COMPLAINT**

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 Nick.com, a website owned by Defendant Viacom Inc., (hereinafter "Viacom") and 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. With neither the knowledge nor the consent of their parents, the Defendants accessed, stored and utilized unique and specific electronic identifying information and content about each of these children 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 website Nick.com.

5. The Defendants utilized Internet technologies commonly known as "cookies" to track and share the Plaintiffs' and putative class members' video-viewing histories and Internet communications on Nick.com without Plaintiffs' informed authorization or 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. Based upon the Defendants' conduct plaintiffs assert 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 New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq.; and

c. Intrusion Upon Seclusion.

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 website Nick.com.

10. 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 website Nick.com.

11. 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.

12. 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.

13. 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.

14. 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.

B. Defendant Viacom

15. Defendant Viacom, Inc. is a publicly-traded Delaware corporation with headquarters at 1515 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.

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

C. Defendant Google

17. 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.

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

18. Google has, by design, become the global epicenter of Internet search and browsing activity. Former Google CEO and current company Executive Chairman Eric Schmidt described Google's privacy plan policy aptly in 2010. "Google's policy," Schmidt said, "is to get right up to the creepy line and not cross it." As detailed below, Google has a history of drawing a line on privacy – and then later crossing right over it.

IV. JURISDICTION AND VENUE

19. 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.

20. 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). 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.

21. 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.

22. 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 Internet Users Access Websites

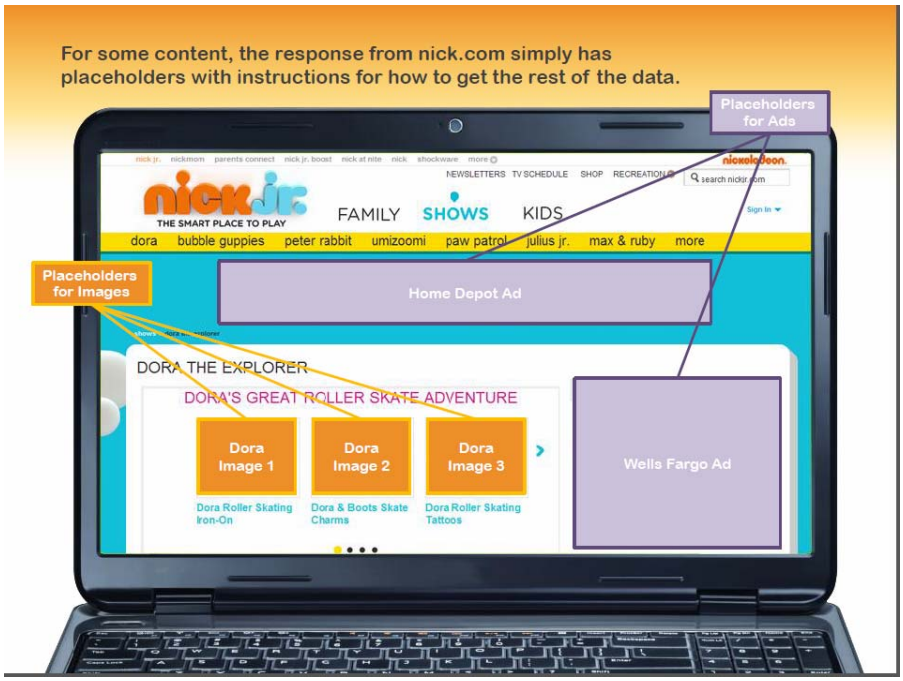
23. In order to access and communicate on the Internet, people employ web-browsers such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

24. 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.

25. The basic command web browsers use to communicate with website servers is called the "GET" command.

26. 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:

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



28. 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.

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

B. How Targeted Internet Advertising Works

30. 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.

31. 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.

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

33. 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.

34. 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.

35. 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.

36. 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 a specific child's Internet history.

37. 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.

38. 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.

39. 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 advertisement for that particular page.

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

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

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. 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.

44. 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 typed the name of a single web page into his or her browser. Graphically, the concept is illustrated as follows:

45. 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. 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 Value of the Personal Information Defendants Collect

46. 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.[2]

47. 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.[3]

48. 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."[4]

49. 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.[5]

50. Upon information and belief, most of the Defendants' advertising clients pay on a

---

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

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

[4] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Business and Policymakers – Preliminary FTC Staff Report*, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37 (last visited October 22, 2013).

[5] 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).

cost-per-click basis.

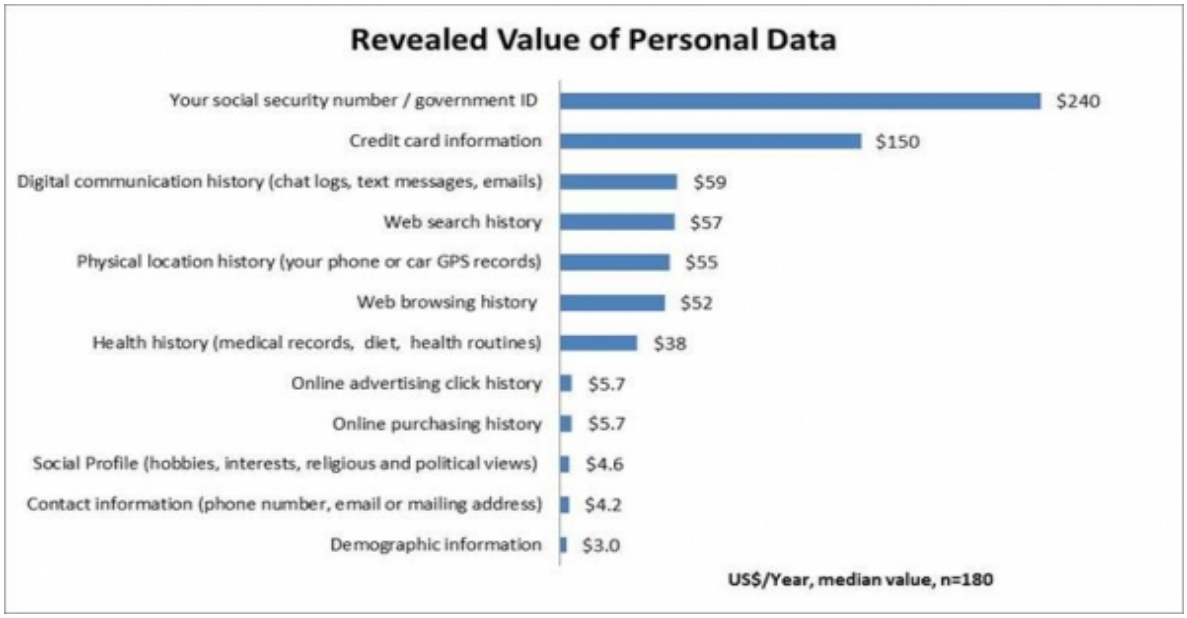
51. The Defendants also offer cost-for-impression ads, which charge an advertising client each time the client's ad displays to a user.

52. 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.[6]

53. 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[7]:

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

[7] 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).



54. 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,[8] 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.[9] Google's Screenwise Trends program demonstrates conclusively that Internet industry participants, including the Defendants, recognize the enormous value in tracking users' Internet communications.

55. Targeting advertisements to children adds *more* value than targeting to adults because children are generally unable to distinguish between content and advertisements. This is especially true in the digital realm where children are less likely to identify and counteract the

[8] 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).

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

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."[10]

56. 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."[11] In particular, Viacom disclosed substantially more information to third-party tracking companies on its children sites than typical adult websites. According to the investigation in September 2010, Viacom placed 92 tracking cookies on the Nick.com website, a total which is 144 percent more than the average number of tracking cookies placed on the 50 most popular adult websites in the United States.[12]

D. Internet Tracking is Not Anonymous

57. 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:

---

[10] 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).

[11] 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).

[12] See http://blogs.wsj.com/wtk-kids/ for statistics on Nick.com and other children's sites (last visited July 30, 2014); see http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 for tracking statistics on the most popular adult websites (last visited July 30, 2014).

> 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.
>
> 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]

58. 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]

59. 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

[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).

categories of data [personally identifiable information and anonymous information] has eroded and is losing its relevance.[15]

60. 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 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]

61. 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]

62. By using browser-fingerprinting alone, the likelihood that two separate users have the same browser-fingerprint is one in 286,777 or 0.000003487 percent.[18] This accuracy is increased substantially where a tracking company also records a user's IP address and unique

---

[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).
[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.
[18] *How Unique Is Your Web Browser?* by Peter Eckersley, available at https://panopticlick.eff.org/browser-uniqueness.pdf (last visited July 28, 2014).

device identifier.

63. 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 targeted ads based on users' behavior.[19]

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

a. 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

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

more."[20] 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."

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

E. Internet Service Provider and Web-Browser Privacy Policies Prohibit Unlawful and Non-Consensual Tracking of User Communications

65. Internet Service Providers (ISPs) provide connection services which allow consumers to send, and receive electronic communications on the Internet. ISPs operate under Privacy Policies that prohibit users from engaging in unlawful or non-consensual tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts. For example, major ISPs such as AT&T, Time Warner, Century Link, Verizon, and Charter all expressly prohibit unlawful acts. [22] Plaintiffs are not aware of any ISP in the United States which consents to the use of its service to engage in criminal or otherwise unlawful

[20] 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).

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

[22] See http://www.corp.att.com/aup/ (last visited July 28, 2014); http://help.twcable.com/twc_misp_aup.html (last visited July 28, 2014); http://www.centurylink.com/Pages/AboutUs/Legal/AcceptableUse/acceptableUsePolicy.jsp (last visited July 28, 2014); https://my.verizon.com/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=AcceptableUse (last visited July 28, 2014); https://www.charter.com/browse/content/policies-comm-acceptable-use (last visited July 28, 2014)

acts.

66. Similarly, web-browsers are software services which allow consumers to send and receive electronic communications on the Internet. Like ISPs, web-browsing services include Terms of Use, which prohibit users from engaging in unlawful or unauthorized tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts. For example, major web-browsers such as Google Chrome, Microsoft Internet Explorer, and Apple Safari all expressly prohibit unlawful acts.[23] Plaintiffs are not aware of any major web-browser which consents to the use of its service to engage in criminal or otherwise unlawful acts.

F. How Viacom and Google Track Children's Internet Use

67. Immediately upon the Plaintiffs' first communication with Nick.com, Defendant Viacom automatically placed its own first-party cookies on the computing devices of the Plaintiffs.

68. Additionally, immediately upon the Plaintiffs' first communication with Nick.com, Viacom knowingly permitted Defendant Google to place its own third-party cookies on the computing devices of the Plaintiffs and then transmitted the Plaintiffs' subsequent communications to Google through those persistent tracking cookies and other information, or, in cases where Google's third-party cookies were already present on the Plaintiffs' computing devices, Viacom transmitted to Google the Plaintiffs' communications through the persistent tracking cookies which already existed on the user's device by virtue of Plaintiffs having visited another website affiliated with Google.

[23] See https://www.google.com/intl/en_US/chrome/browser/privacy/eula_text.html (last visited July 28, 2014); http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/end-user-license-agreement (last visited July 28, 2014); and http://www.apple.com/legal/sla/docs/SafariWindows.pdf (last visited Sept. 10, 2014).

69. Viacom allowed Google to place and access cookies from its doubleclick.net domain.

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

71. 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 access to the Plaintiffs' Internet communications.

72. Google's third-party cookies tracked with a unique persistent cookie identifier, among other things, the URLs (Uniform Resource Locators) visited by the Plaintiffs, the Plaintiffs' respective IP addresses, browser settings, unique device identifiers, operating systems, screen resolutions, browser versions, detailed video viewing histories and the details of their Internet communications with Nick.com.

73. A URL is composed of several different parts.[24] 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;

[24] 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).

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". Graphically, the concept is illustrated as follows:

74. The URLs visited by plaintiffs and putative class members contain substantive and often sensitive content. For example:

a. A Plaintiff minor child seeking information about "what to do if my parents are getting divorced" may enter that search term in the Google search engine.

b. The second result in Google's search engine is a hyperlink with the Subject Line: "How to Deal With Your Parents' Divorce: 12 Steps."

c. By clicking on the link and affirmatively indicating through the web-browser that they seek information on their parents' divorce, the browser would send a communication on the Plaintiffs' behalf to a webpage with the URL, http://www.wikihow.com/Deal-With-Your-Parents'-Divorce.

d. In response to the Plaintiffs' "GET" request communication seeking information on what to do if their parents get divorced, the website WikiHow.com returns a communication which includes an essay with 12 detailed steps a child could take if their parents were getting a divorce.

e. Google places cookies on WikiHow.com with the same unique identifiers as the cookies placed on the Viacom children's websites.

75. Similarly, for the URL, http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html, 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: in particular an episode of the show Penguins of Madagascar titled "Skipper's Nightmare."

76. On Nick.com, Viacom further disclosed to Google at least the following about each Plaintiff who was a registered user of Nick.com: (1) the child's username/alias; (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; (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; and (11) the DoubleClick persistent cookie identifiers.

77. By disclosing the above information to Google, Viacom has knowingly disclosed

information which, without more, when disclosed to Google, links specific persons with their online communications and data, based on information that Google already has in its possession.

G. How Google Identifies Specific Individuals and Their Families

78. Defendant Google publicly admits 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.[25]

79. Google has a ubiquitous presence on the Internet. In October 2012, DoubleClick cookies were present on 69 of the 100 most popular websites.[26] In July 2013, experts estimated Google accounted for 25 percent of all Internet traffic running through North American ISPs, an amount larger than the combined traffic of Facebook, Netflix, and Instagram.[27] In addition to DoubleClick, Google owns and operates:

a. The world's third most popular social network at plus.google.com,[28] for which Google claims to have over 300 million users;

b. The world's most popular search engine at Google.com, which, according to comScore, processed 12.1 billion searches in the United States in June 2014, or 68 percent of all U.S. Internet searches.[29]

---

[25] Google.com Google Developer Cookie Guide, https://developers.google.com/adexchange/rtb/cookie-guide (last visited September 16, 2013).
[26] See http://www.law.berkeley.edu/privacycensus.htm (last visited July 24, 2014).
[27] See http://www.wired.com/2013/07/google-internet-traffic/ (last visited July 29, 2014).
[28] According to Alexa, Facebook and LinkedIn have more users than Google Plus.
[29] See https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-June-2014-US-Search-Engine-Rankings (last visited July 29, 2014).

c. The world's most popular email service at Gmail.com, which, as of June 2012, had more than 250 million users worldwide;[30]

d. The world's most popular video service at YouTube.com, which, according to comScore, had 153 million unique video viewers in June 2014;[31]

e. A mapping service called Google Maps at www.google.com/maps that includes applications which track the precise geo-locations of users, and which is according to some estimates, the most popular smartphone app in the world;

f. An online personal photography website called Picasa at picasa.google.com;

g. Its own electronic store called Play at play.google.com;

h. Its own web-browser called Google Chrome;

i. An online software suite called Google Apps that, as of June 2012, was used by 66 of the top 100 universities in the United States, government institutions in 45 states, and a total of 5 million businesses;[32] and

j. Android, its mobile phone platform is the most highly used platform in the United States and allows Google to track user movements, app usage, and phone calls.

80. Google collects users' IP addresses, unique device identifiers, and user account information through all of the services listed above. In addition, it tracks use of these services

[30] See http://googleblog.blogspot.com/2012/06/chrome-apps-google-io-your-web.html (last visited July 24, 2014).
[31] See http://ir.comscore.com/releasedetail.cfm?ReleaseID=860971 (last visited July 29, 2014).
[32] *Id*.

with persistent cookie identifiers. For example:

a. Google's social-network at Google Plus tracks users with cookies from DoubleClick with the same persistent identifier it uses to track at Nick.com. In addition to DoubleClick cookies, Google tracks its social network users with cookies from plus.google.com, clients6.google.com, and talkgadget.google.com.

b. Google's search engine tracks users with cookies from the main Google.com domain and from Google's social network at plus.google.com.

c. Google's email service at Gmail tracks users with cookies from mail.google.com and from Google's social network at plus.google.com.

d. Google's video service at YouTube.com tracks users with cookies from DoubleClick with the same persistent identifier that it uses to track each user at Nick.com. In addition to DoubleClick cookies, Google tracks YouTube users with cookies from its social network at plus.google.com, apis.google.com, gg.google.com, and clients6.google.com.

e. Google's map service tracks users with cookies from google.com and receives precise geo-location data from users utilizing its mapping services.

f. Google's electronic storage service called Drive tracks users with cookies from its social network at plus.google.com, and the subdomains drive.google.com and docs.google.com.

g. Google's electronic store Play tracks users with cookies from its social

networking site at plus.google.com.

81. Use of Gmail and the social network Google Plus requires registration, a process through which Google obtains a user's first and last name, hometown, email address, and other personal information about each user.

82. Other Google services collect users' first and last names, hometowns, email addresses, and other personal information when the user signs up as a member for those services.

83. Google admits that it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user account information. Its current privacy policy states that:

a. It "may collect device-specific information (such as [a user's] hardware model, operating system version, unique device identifiers, and mobile network information including phone number)" and "may associate … device identifiers or phone number[s] with [a user's] Google Account."[33]

b. It may "automatically collect and store certain information in server logs. This may include: … search queries, … Internet protocol address, … device event information such as … hardware settings, browser type, browser language, the data and time of your request and referral URL," and "cookies that may uniquely identify your browser or your Google Account."[34]

84. Google's current Privacy Policy is substantially similar to the one in effect at the time the Plaintiffs' initially filed suit in this case regarding its collection of information. The policy in effect at the time Plaintiffs' filed suit provided as follows:

[33] See http://www.google.com/policies/privacy/ (last visited July 24, 2014).
[34] Id.

Device information
We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

Log information
When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

- details of how you used our service, such as your search queries.
- telephone log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account.

Location information
When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

Unique application numbers
Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

Local storage
We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

Cookies and anonymous identifiers
We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

85. Google's Privacy Policy in effect today differs in one key respect from the Policy

in effect at the time Plaintiff's filed suit in this case. Google's current Privacy Policy acknowledges that it has the information to connect DoubleClick cookie information with personal information collected from its other services, but promises not to. Google informs users:

> We may combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

86. Google's Privacy Policy promise not to combine DoubleClick cookie information with personally identifiable information was not in place until March 1, 2012.[35] Because Plaintiffs filed suit in December 2012, Viacom's disclosures to Google were made for a significant period of time without any public commitment by Google that it would not use the information disclosed by Viacom.

87. On March 1, 2012, Google publicly announced that it would be commingling information obtained from Google users across Google accounts. In a company blog post by Alma Whitten, Google's Direct of Privacy, Product, and Engineering, the company announced:

> Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products[.][36]

88. In addition to these websites and services listed above, Google advertises a "cookie matching" service for ad-buyers that permits buyers to match their own cookie with a DoubleClick persistent cookie identifier assigned to a user by Google.

89. Defendant Google admits that IP addresses and cookie information are not

[35] The changes to Google's Privacy Policy as of March 1, 2012 are highlighted here: http://www.google.com/policies/privacy/archive/20111020-20120301/ (last visited July 24, 2014).

[36] See http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html. (last visited July 25, 2014).

anonymous to Google. In fact, Google promises users it will scrub full IP addresses and cookie information from its records after 9 or 18 months in order to "anonymize" user data:

> Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. *We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).* If you have Search History enabled, this data may also be stored in your Google Account until you delete the record of your search. *Emphasis added.*

90. Google has further admitted that IP addresses are personal information where the IP address is capable of being tied to an individual by a company. On Google's Public Policy blog in 2008, then Google software engineer Alma Whitten explained:

> [I]s an IP address personal data, or, in other words, can you figure out who someone is from an IP address? A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you're an ISP and you assign an IP address to a computer that connects under a particular subscriber's account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings.[37]

91. Google has more information about Internet users than the ISPs identified by Whitten. Each separate Google product logs and keeps track of different categories of information about Internet users, including, but not limited to the following list:

a. first and last names,

b. home or other physical address,

c. precise current locations of users through GPS,

[37] See http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (last visited July 24, 2014).

d. IP addresses,

e. telephone numbers,

f. lists of contacts,

g. the content of Gmail users' Gmail messages,

h. search history at Google.com and YouTube,

i. web-surfing history,

j. Android device activity, and

k. all activity on Google's social network called Google Plus.

92. In the case of Nick.com, Google occupies the role of the ISP because it knows its users' full names, hometowns, specific geographic locations, email addresses, and more.

93. Viacom is aware of Google's ubiquitous presence on the Internet and its tracking of users across DoubleClick partner websites like Nick.com and Google's own websites at Google.com, Google Plus, YouTube.com, Gmail.com, and Play.Google.com, among others, where Google connects user IP addresses, unique device identifiers, and persistent cookie identifiers to Google account information.

94. As a result of Google's ubiquitous presence on the Internet, the information Viacom discloses to Google personally identifies the plaintiffs.

H. Google's Internal Position on Privacy.

95. Despite Google's promise not to connect DoubleClick information with Google Account information, Google reserves the right to change its Privacy Policy "from time to time" and has a history of exercising this provision. For example, its March 2012 announcement that it would commingle user information across Google accounts broke promises it had previously made with respect to Android, Google search, and Gmail.

96. Prior to March 2012, Google did not give any public indications that it was in the process of changing company policy to commingle all user data across its Search, Gmail, YouTube, Maps, Docs, Picasa, Play, Android, and other services. But this shift to share information across all Google platforms actually began at least as early as May 2010, when Google executives decided to engage in a plan it called "Emerald Sea" which involved eliminating then existing barriers between Google properties.

97. "Emerald Sea" was driven in large part by the Google's desire to better compete with Facebook to create detailed digital dossiers of its users.

98. James Whittaker, a former Google Engineering Director, described Google's motivation in a public explanation of his resignation from the company:

> It turns out that there was one place where the Google innovation machine faltered and that one place mattered a lot: competing with Facebook. … Like the proverbial hare confident enough in its lead to risk a brief nap, Google awoke from its social dreaming to find its front runner status in ads threatened. … Google could still put ads in front of more people than Facebook, but Facebook knows so much more about those people.
>
> Advertisers and publishers cherish this kind of personal information, so much so that they are willing to put the Facebook brand before their own. Exhibit A: www.facebook.com/nike, a company with the power and clout of Nike putting their own brand after Facebook's? No company has ever done that for Google and Google took it personally.

99. Unlike Facebook, prior to the commingling of information and creation of Google Plus, Google could not create nearly as total a picture of its users for advertisers.

I. Viacom Disclaims Any Control Over Use of Information It Discloses to Google

100. In its own Privacy Policy for Nickelodeon websites that Viacom filed as Exhibit D in response to Plaintiff's' First Consolidated Complaint (and which is not valid for the minor children plaintiffs in this case or for purposes of the VPPA), Viacom disavows any control over Google's practices, stating that "the use of [tracking] technology by these third parties is within

their control and not the Nickelodeon sites. Even if we have a relationship with a third party, we do not control those sites or their policies and practices regarding your information[.]"

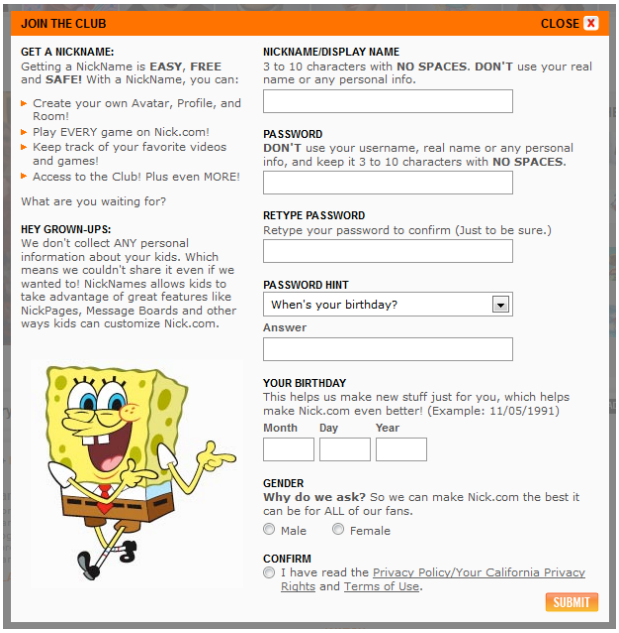
J. Viacom's Disclosures to Google are Not Necessary for Nick.com

101. Google's DoubleClick cookies are not necessary for Viacom to render any services on Nick.com. On or about August 1, 2014, Viacom revamped its Nick.com website. As of August 7, 2014, based on Plaintiffs' investigation, Defendant Viacom no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google.

K. What Viacom and Google Knew About the Age and Gender of Viacom Users

102. Upon arriving at Nick.com, Viacom encouraged its users to register and establish profiles for those websites.

103. During the registration process, Viacom obtained the birthdate[38] and gender of its users, through the following sign-up form:



[38] Plaintiffs note that this accurate sign-up form differs from the purported sign-up form Viacom offered as an Exhibit A attached to their previous Motion to Dismiss, which was not an accurate depiction of the sign-up process at the time the plaintiffs' filed suit. This version requires an exact birthdate for a child to create an account.

104. Viacom gave its users an internal code name based upon their answers to the gender and birth date questions. For instance, Viacom gave 6 year-old males the code name "Dil", and 12 year-old males the code name "Lou". Viacom calls this coding mechanism the "rugrat" code. 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.

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

106. Viacom disclosed to Google each child's profile name and the code name for the child's specific gender and age.

107. Through these disclosures and the disclosure of the persistent cookie identifiers of the DoubleClick.net cookies, and the Plaintiffs' IP address, browser settings, and other information explained above, Viacom knowingly disclosed to Google information which, without more, when disclosed to Google, itself links the actual plaintiffs to specific video materials for Defendant Google based on information Google already has in its control.

G. How Viacom Disclosed the Plaintiff Minor Children's Video Viewing Histories

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

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

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

111. For instance, the following video viewing activity of a Nick.com user would be 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_shorts_skippers_nightmare***[39];sec0=clbu;sec1=clubhouses;sec2=penguins_of_madagascar;cat=2;***rugrat=Dil***[40];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])***

112. 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. Viacom also disclosed each individual plaintiff's username to Google that was input when a child logged-in or visited his or her profile page, a process through which 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.

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

114. 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

115. 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:

> **U.S. Resident Class**: All children under the age of 13 in the United States who visited the website Nick.com and had Internet cookies that

[39] *Penguins of Madagascar: Skipper's Nightmare* is the name of the video requested by this user.
[40] "Dil" is the code name Viacom gives to male users, age 6.

> 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 and who engaged with one or more video materials on such site, and who had their video viewing histories knowingly disclosed by Viacom to Google.

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

117. 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.

118. 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 users.

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

e. Whether or not Viacom should be enjoined from further disclosing information about the video materials its minor children users watch on its sites; Whether the Defendants intruded upon the Plaintiffs' seclusion;

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

g. Whether punitive damages are appropriate.

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

121. 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.

122. 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 Defendants' 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.

123. 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.

124. 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.

125. 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.

126. 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

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

128. The Video Privacy Protection Act, 18 U.S.C. § 2710, (hereinafter "VPPA") prohibits a video tape service provider from knowingly disclosing personally identifiable information concerning any consumer of such provider to a third-party without the informed written consent of 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 open-ended and "includes information 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."

d. There is no exception in the VPPA for disclosures to a third party which publicly promises not to use personally identifiable information.

e. 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 at the time the disclosure is sought." [41]

129. As amended in December 2012, the VPPA creates an opt-out right for consumers. It requires VTSPs that disclose personally identifiable information with the "informed, written consent" of the consumer to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." 18 U.S.C. § 2710(2)(B)(iii).

130. The Video Privacy Protection Act of 1988 was passed for the explicit purpose of protecting the privacy of individuals' and their families' video requests and viewing histories. As explained in the Senate report for the Act, "The impetus for this legislation occurred when a weekly newspaper in Washington published a profile of Robert H. Bork based on the titles of 146 files ***his family had rented*** from a video store." S.Rep. 100-599 at 6 (1988).

131. 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

[41] 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."

> 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).

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

> 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).

133. 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."[42]

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

[42] 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)

> 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.

135. The legislative history of the VPPA provides that Congress understood technology would soon make tracking "relatively easy" and the intent of the VPPA was to keep up with technology:"Unlike the other definitions in [the VPPA], paragraph (a)(3) uses the word 'includes' to establish a minimum, but not exclusive definition of personally-identifiable information." S. Rep. 100-599 at 12 (1988).

136. Congress recognized the definition of PII for children's use of the Internet in the legislative history to the 2012 amendments:

> This Committee does not intend for this clarification to negate in any way existing laws, regulations, and practices designed to protect the privacy of children on the Internet. …
>
> Website operators … share in the responsibility to protect consumer privacy, particularly the privacy of children. To facilitate this goal, Congress enacted the Children's Online Privacy Protection Act effective April 21, 2000, which applies to the online collection of personal information from children under 13. Compliance with the Act is overseen by the Federal Trade Commission, which enacted rules governing web site operator compliance, including a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online.
>
> …
>
> The Act and its regulations apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information – for example, hobbies, interests, and information collected through cookies and other types of tracking mechanisms – when they are tied to individually identifiable information.

H. Rep. 112-312 at 3-4 (2011).

137. The information at issue in this case fits the current real-world definition of "personally identifiable information." For example:

a. IP addresses, unique device identifiers, persistent cookie identifiers, browser-fingerprints, and usernames/aliases can all be used to identify or contact a person – particularly when the entity to which such information is disclosed is the world's largest Internet company and tracks users' real names, addresses, geo-locations, phone numbers, contacts, and behavior across a suite of the world's most popular Internet services.

b. Both Defendants Viacom and Google are members of the Interactive Advertising Bureau and agree to comply with the IAB's Code of Conduct. In particular, Viacom and Google publicly promise through IAB membership that they will "not collect 'personal information' as defined in the Children's Online Privacy Protection Act ('COPPA'), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising direct to children they have actual knowledge are under the age of 13 except as compliant with the COPPA." For children, the data tracking industry defines "personal information" as it is defined in the Children's Online Privacy Protection Act where the tracking company "has actual knowledge" that the child is under the age of 13 or where the tracking is done on a website direct to children under the age of 13.

c. The Federal Trade Commission, after extensive hearings, and in its fact-finding role regarding regulation of children's use of the Internet, found that persistent identifiers are PII:

> The Commission continues to believe that persistent identifiers permit the online contacting of a specific individual. As the Commission stated in the 2011 NPRM, it is not persuaded by arguments that persistent identifiers only permit the contacting of a device. This interpretation ignores the reality that, at any given moment, a specific individual is using that device. Indeed, the whole premise underlying behavioral advertising is to serve an advertisement based on the perceived preferences of the individual user.
>
> Nor is the commission swayed by arguments noting that multiple individuals could be using the same device. Multiple people often share the same phone number, the same home address, and the same email address, yet Congress still classified those, standing alone, as "individually identifiable information about an individual." For these reasons, and the reasons stated in the 2011 NRPM, the Commission will retain persistent identifiers within the definition of personal information.

138. 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.

139. 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).

140. The VPPA also clearly applies to online VTSPs that show television or other video programs. As explained in the legislative history to the 2012 amendments:

> When this law was originally enacted in 1988, consumers rented movies from brick-and-mortar video stores such as Blockbuster. Today, not only are VHS

> tapes obsolete, so too are traditional video rental stores. The Internet has revolutionized how consumers rent and watch movies and television programs. Video stores have been replaced with "on-demand" cable services or Internet streaming services that allow a customer to watch a movie or TV show from their laptop or even their cell phone.
>
> H. Rep. 112-312 at 2 (2011).
>
> At the time of the VPPA's enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988 – the VHS cassette tape – is now obsolete. In its place, the Internet has revolutionzed the way that American consumers rent and watch movies and television programs. Today, so-called "on demand" cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.
>
> S. Rep. 112-258 at 2 (2012).

141. 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 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 as of the time Plaintiffs' originally filed this suit. *See* Nick.com (September 24, 2013).

142. Plaintiffs and members of the putative video sub-class are "consumers' under the VPPA in that they are registered users of Nick.com, and therefore, constitute subscribers to the video services Viacom provides on Nick.com.

143. Viacom disclosed to Google at least the following about each Plaintiff who was a registered user of Nick.com: (1) the child's username/alias; (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; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers.

144. By disclosing the above information to Google, Viacom knowingly disclosed information which, without more, when disclosed to Google, links specific persons with their video requests and/or viewing histories based on information that Google already has in its possession.

145. Viacom violated the VPPA by knowingly disclosing to Google information which, without more, when disclosed to Google, links specific persons with their video requests and viewing histories based on information that Google already has in its possession.

146. 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.

147. Viacom further violated the VPPA after passage of the amended VPPA by failing to provide plaintiffs with the opt-out right codified in the amended VPPA in 18 U.S.C. § 2710(2)(B)(iii).

148. On or about August 1, 2014, Defendant Viacom revamped its Nick.com website. As of August 7, 2014, based on Plaintiffs' investigation, Defendant Viacom no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google.[43]

149. As a result of the above violations and pursuant to 18 U.S.C. § 2710, the

[43] Though Plaintiffs' investigation did not reveal the continued disclosure of information from Viacom to Google, plaintiffs' note that they have not had opportunity for discovery to determine whether disclosures between the defendants continue to occur that is not detectable from the plaintiffs' individual computers.

Defendant Viacom is 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 Defendant in the future."

COUNT II – NEW JERSEY COMPUTER RELATED OFFENSES ACT

U.S. Resident Children v. All Defendants

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

151. 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.

152. 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.

153. Specifically, Defendants accessed Plaintiffs' and Class Members' computers in order to illegally harvest Plaintiffs' and Class Members' personal information. Through conversion and without consent, Defendants harvested Plaintiffs' personal information for their unjust enrichment and to the financial detriment of Plaintiffs and Class Members. Had Plaintiffs, Class Members, and/or their parents and/or guardians known that Defendants were converting Plaintiffs' personal information for financial gain, Plaintiffs, Class Members, and/or their parents and/or guardians would have at least expected remuneration for their personal information at the time it was conveyed.

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

155. 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.

156. 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 III – INTRUSION UPON SECLUSION

U.S. Resident Children v. All Defendants

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

158. 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.

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

160. The Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion is highly offensive to a reasonable person in that Defendants' conduct violated federal and state civil and criminal statutes designed to protect individual privacy. Specifically, the Defendants' conduct violated:

a. The Video Privacy Protection Act as alleged above;

b. The Wiretap Act because they engaged in a scheme to intentionally intercept the contents of the minor Plaintiffs' electronic communications without their or their guardians' consent;

c. In the alternative to finding that Defendants' conduct violated the Wiretap Act, this Court must find that the Defendants' conduct violated the Pen Register Act, 18 U.S.C. 3121, et seq., which makes it a federal crime for any person to "install or use a pen register or trap and trace device" without the consent of the user of an electronic communication service. A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3). A "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to

identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4). Violation of the Pen Register Act is subject to imprisonment for one year.

d. The Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants knowingly placing or facilitated the placement of third-party cookies on the computing devices of minor children who were not aware of and could not consent to their placement, thereby intentionally exceeding authorized access to the Plaintiffs' computers and obtaining information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime statutes of all 50 states.

161. Defendants' actions in committing criminal acts which violated the privacy rights of millions of American children is highly offensive to a reasonable person.

162. Defendants' unauthorized tracking of the minor children Plaintiffs' communication on the Internet, including, as detailed above, communications on sensitive topics, such as divorce and health URLs, is highly offensive to a reasonable person.

163. The Defendants' intentional intrusion on the Plaintiffs' solitude and seclusion violated the Terms of Use of both the Internet Service Providers and the web-browsers employed by the Plaintiffs, which prohibit the use of those services in criminal activity, unlawful activity, and the tracking of Internet communications without consent.

164. In December 2012, the same month plaintiffs initially filed their respective suits,

the Center for Digital Democracy surveyed more than 2,000 adults about basic principles of children's online privacy.[44] When asked whether they agreed or disagreed with the following statements, the polled adults responded as follows:

a. "It is wrong for advertisers to collect and keep information about where a child goes online and what that child does online."

- 45 percent strongly agree
- 13 percent somewhat agree
- 12 percent somewhat disagree
- 27 percent strongly disagree
- 3 percent do not know or refused to answer

b. "It is okay for advertisers to track and keep a record of a child's behavior online if they give the child free content."

- 5 percent strongly agree
- 6 percent somewhat agree
- 16 percent somewhat disagree
- 70 percent strongly disagree
- 3 percent do not know or refused to answer

c. "As long as advertisers don't know a child's name and address, it is okay for them to collect and use information about the child's activity online."

- 4 percent strongly agree
- 14 percent somewhat agree
- 13 percent somewhat disagree
- 67 percent strongly disagree
- 2 percent do not know or refused to answer

d. "Before advertisers put tracking software on a child's computer, advertisers should receive the parent's permission."

- 82 percent strongly agree

[44] The survey is available at http://www.centerfordigitaldemocracy.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf (last visited July 25, 2014).

- 9 percent somewhat agree
- 2 percent somewhat disagree
- 4 percent strongly disagree
- 2 percent don't know or refused to answer

e. When asked, "There is a federal law that says that online sites and companies need to ask parents' permission before they collect personal information from children under age 13. Do you think the law is a good idea or a bad idea?" 90 percent said it was a good idea, 7 percent said it was a bad idea, and 2 percent did not know or refused to answer.

f. Parents in the survey were more protective of children's privacy than non-parents.

g. In connection with an investigation of cookie tracking on children's websites, the Wall Street Journal asked readers:

"How concerned are you about advertisers and companies tracking your behavior across the web?" An overwhelming majority of respondents indicated concern.

- 59.7 percent said they were "very alarmed"
- 25 percent said they were "somewhat alarmed"
- 3.7 percent said they were "neutral"
- 7 percent said it was "not a big worry"
- 4.5 percent said they "could not care less"[45]

h. In November 2012, the Washington Post asked Americans:[46]

"How concerned are you, if at all, about the government or private companies collecting digital information from your computer or phone?"

[45] See http://blogs.wsj.com/wtk-kids/ (last visited July 30, 2014).
[46] See http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/12/21/National-Politics/Polling/question_12669.xml?uuid=FuyJGmqMEeOZe5ITsX2slw (last visited July 30, 2014).

- 43 percent were "very concerned"
- 26 percent were "somewhat concerned"
- 18 percent were "not too concerned"
- 12 percent were "not at all concerned," and
- 1 percent had "no opinion"

How concerned are you, if at all, about the collection and use of your personal information by websites like Google, Amazon, or Ebay?

- 37 percent were "very concerned"
- 32 percent were "somewhat concerned"
- 17 percent were "not too concerned"
- 13 percent were "not at all concerned"
- 2 percent had "no opinion"

i. In Winter 2012, the Pew Research Center on the Internet and American Life asked Americans: "Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online – even if neither is exactly right?"

- 68 percent said, "I'm not okay with it because I don't like having my online behavior tracked and analyzed."
- 28 percent said, "I'm okay with it because it means I see ads and get information about things I'm really interested in."
- 4 percent said "neither" or "don't know."

165. Defendants' actions were highly offensive to a reasonable person for each plaintiff individually, and this offensiveness is made worse because the acts were perpetrated literally millions of times on millions of children.

166. Defendants actions were highly offensive to a reasonable person because Defendants' targeting of children was more intrusive in that the defendants placed significantly more tracking technologies on children's websites than adult websites to take advantage of the Plaintiffs' vulnerability as children.

167. Defendants' actions were highly offensive to reasonable people because they

violated the online advertising industry and their own standards for respecting the personal information of children.

168. As a result of the above, the Defendants are liable to the Plaintiffs and the Class for general damages to the Plaintiffs' interest in privacy resulting from the invasions, compensatory and punitive damages.

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: September 11, 2014

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

BARTIMUS, FRICKLETON, ROBERTSON & GOZA 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