Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
Children's Online Privacy Protection Rule:	)	Project No. P-104503
	)	
Request for Public Comment on Proposal to Amend Rule to Respond to Changes in Online Technology	)	

COMMENTS OF

The Center for Digital Democracy,
American Academy of Child and Adolescent Psychiatry,
American Academy of Pediatrics,
Benton Foundation,
Berkeley Media Studies Group/Public Health Institute,
Center for Commercial-Free Childhood,
Center for Science in the Public Interest,
Children Now,
Consumer Action,
Consumer Federation of America,
Consumer Watchdog,
Praxis Project,
Privacy Rights Clearinghouse,
Public Health Advocacy Institute at Northeastern University School of Law,
Public Health Law and Policy,
Rudd Center for Food Policy & Obesity at Yale University, and
World Privacy Forum

Of counsel:

Ariel Gursky
Law Student
Georgetown Law

Angela J. Campbell,
Laura M. Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535

Dated: December 23, 2011

Counsel for Center for Digital Democracy

TABLE OF CONTENTS

I. Dramatic Growth in the Children's Digital Marketplace, Along with Increasingly Sophisticated Tracking and Targeting Practices, Make it Imperative that COPPA Be Updated. 1

II. Children's Privacy Advocates Generally Support the Proposals to Clarify and Update the Definitions in the COPPA Rule 17

A. Overview of Proposed Changes 17

1. Definitions of "Personal Information" and "Support for Internal Operations" 18
2. Definition of "Collects or Collection" 19

B. Persistent Identifiers Must Be Included in the Definition of Personal Information 20

1. New Research Reveals Widespread Tracking and Behavioral Advertising on Websites Most Popular with Children 21
2. Operators Employ Methods of Tracking and Behavioral Advertising on Children's Websites 22
3. The Inclusion of Persistent Identifiers Is Necessary to Protect Children 26

C. Personal Information Should Include Screen and User Names 28

D. Personal Information Should Include Geolocation Information 29

E. Personal Information Should Include Photographs, Videos, and Audio Files 32

F. The Definition of Personal Information Should Include Both ZIP+4 and the Combination of Date of Birth, Gender and ZIP Code 33

III. The Commission Should Adopt Most of the Proposed Revisions to Notice Requirements and Consent Mechanisms 34

A. CDD Supports Making Notice Requirements More Helpful to Parents 36

1. Children's Privacy Advocates Support Clarification that All Operators Must Provide Online Notice 36
2. Children's Privacy Advocates Support the Proposal to Simplify Online Privacy Policies with Some Exceptions 39
3. Children's Privacy Advocates Support Proposals for Just-in-Time Direct Notice to Parents 40

B. Children's Privacy Advocates Generally Support the Proposed Revisions to Consent Mechanisms 41

IV. The Commission Should Adopt Limits on Data Retention 42

V. Self-Regulatory Efforts Are Insufficient to Protect Children's Privacy 43

Conclusion 45

The Center for Digital Democracy, American Academy of Child and Adolescent Psychiatry, American Academy of Pediatrics, Benton Foundation,[1] Berkeley Media Studies Group/Public Health Institute, Center for Commercial-Free Childhood, Center for Science in the Public Interest, Children Now, Consumer Action, Consumer Federation of America, Consumer Watchdog, Praxis Project, Privacy Rights Clearinghouse, Public Health Advocacy Institute at Northeastern University School of Law, Public Health Law and Policy, Rudd Center for Food Policy & Obesity at Yale University, and World Privacy Forum (collectively "Children's Privacy Advocates") are pleased with the Federal Trade Commission's proposed revisions to the Children's Online Privacy Protection Rule ("COPPA Rule"). This revision of the Rule is an important step in ongoing efforts to protect children on the Internet.

I. Dramatic Growth in the Children's Digital Marketplace, Along with Increasingly Sophisticated Tracking and Targeting Practices, Make it Imperative that COPPA Be Updated.

For more than a decade, the Children's Online Privacy Protection Act (COPPA) has served as an effective safeguard for young consumers under the age of 13 in the online marketing environment. Because the legislation was passed during the early stages of Internet e-commerce, it established a clear set of "rules of the road" to help guide the development of the children's digital marketplace. As a result, operators of child-oriented websites ceased some of the most troubling information collection practices that were commonplace prior to COPPA's passage.[2] The law established an important regulatory

[1] The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

[2] *See* Kathryn C. Montgomery, Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet, 67-106 (MIT Press 2007). A recent study in the *Journal of Consumer Affairs* found that more than 95 percent of the top 100 children's websites in

framework for commercial practices on children's websites. Because of longstanding research documenting children's developmental vulnerabilities to the persuasive techniques of advertisers,[3] one of COPPA's key goals was to prevent online companies from targeting individual children with personalized marketing messages.[4] In keeping with fair information principles, COPPA was also intended to minimize the collection of personal data from children, and to eliminate the practice of offering prizes and other incentives to encourage such data collection.[5] Congress designed COPPA's basic framework to be flexible, anticipating the continued growth of digital media, and requiring the FTC to update its rules in order to ensure that the law's implementation would cover new data collection and marketing practices.[6]

---

the United States post privacy policies complying with COPPA's requirements for information collection and use. Andrea J. S. Stanaland, May O. Lwin, & Susanna Leong, *Providing Parents with Online Privacy Information: Approaches in the US and the UK*, 42 J. Consumer Affairs 474, 484–85 (2009); *see also* Anthony D. Miyazaki, Andrea J. S. Stanaland, & May O. Lwin, *Self-Regulatory Safeguards and the Online Privacy of Preteen Children*, 38 J. Advertising 79, 83 (2009).

[3] Dale Kunkel, *The Role of Research in the Regulation of U.S. Children's Television Advertising*, 12 Science Communication 101 (1990); *see also* Deborah Roedder John, *Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research*, 26 J. Consumer Research 183 (1999).

[4] 144 Cong. Rec. S8483 (statement of S. Richard Bryan).

[5] *See* Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 Fed. Reg. 22,750, 22,758 (Apr. 27, 1999) ("The purpose of [16 C.F.R. pt. 312.7] is to encourage a child's access to activities, but to prevent operators from tying collection of personal information to such popular and persuasive incentives as prizes or games.") [hereinafter 1999 NPRM].

[6] *See Children's Online Privacy Protection Act of 1998: Hearing on S. 2326 Before the Subcomm. on Communications of the S. Comm. on Commerce, Science, & Transportation*, 105th Cong. 7 (1998) (statement of Robert Pitofsky, Chairman, Fed. Trade Comm'n) ("The path taken in S. 2326 . . . provides the FTC with rulemaking authority necessary to implement these provisions in a flexible manner. It takes into account rapid changes occurring in the industry and, importantly, through an innovative safe harbor provision, provides both incentives for industry self-regulation programs and the means for ensuring broadbased implementation of these self-regulatory standards once they are adopted.").

By addressing some of the initial concerns of parents about the online environment, COPPA helped pave the way for a flourishing digital marketplace for young people. As of the first quarter of 2011, the children's online market comprised more than 20 million 2–11 year olds, with children frequenting numerous child-oriented websites, including Nick.com, Miniclip, Poptropica, Webkinz, Disney, and Barbie.com.[7] Children continue to be a lucrative market for advertisers, with ad time on TV and new media platforms generating record sales.[8] Young people between the ages of 8 and 15 control $43 billion in spending annually. Children are also using new media technologies at an earlier age, and spending increasing amounts of time engaged in an expanding array of new platforms, including virtual worlds, interactive games, and mobile apps.[9] As *Adweek* reported, "80 percent of kids under the age of 5 use the Internet weekly, and 60% of kids 3 and younger are now watching videos online."[10] Some 10 percent of 6–8 years olds, 23 percent of 9–10 year olds, and 41 percent of children aged 11–12 are social network users, according to *eMarketer*.[11] Today, by age 11, half of kids have cell phones, according to research released this year by LMX Family/Ipsos OTX. That same report,

---

[7] comScore, *Entertainment-Kids, Q1, 2011*; *see also An Upcoming Change to comScore US Weighting*, comScore U.S. Client Newsletter – August 2011 Edition, http://www.comscore.com/newsletter/2011/August/US_Client_Newsletter#story4 (describing comScore's analysis of the online children's market).

[8] *See* Anthony Crupi, *Upfront: The Kids Are All Right: Younger Set's Bizarre Expected to Top $1 Billion*, Adweek (Mar. 28, 2011), http://www.adweek.com/news/advertising-branding/upfront-kids-are-all-right-126382.

[9] "A child's first cell phone, first game system and his or her exposure to technology are all happening earlier," according to Donna Sabino, senior vice president of Kids and Family Insights at Ipsos OTX Media CT. Wendy Goldman Getzler, *Co-Entertainment, Media Mutlitasking on the Rise*, Kidscreen (Apr. 13, 2011), http://kidscreen.com/2011/04/13/co-entertainment-media-multitasking-on-the-rise/.

[10] Brian Braiker, *The Next Great American Consumer: Infants to 3-Year-Olds: They're a New Demographic Marketers Are Hell-Bent on Reaching*, Adweek (Sept. 26, 2011), http://www.adweek.com/news/advertising-branding/next-great-american-consumer-135207 (citing Aviva Lucas Gutnick, et al., *Always Connected: The New Digital Media Habits of Young Children*, Joan Ganz Cooney Center (Mar. 2011), *available at* http://joanganzcooneycenter.org/Reports-28.html).

[11] *US Child Social Network Users, by Age*, eMarketer (Feb. 2011).

explained *Advertising Age,* noted that "pre-schoolers [are] adopting digital habits or being exposed to new devices even faster than tweens, a sign of the speed with which digital technology is reshaping media and marketing habits for the youngest children."[12]

The dramatic growth of the digital marketplace and its increasing role in the lives of children make it imperative that the rules for implementation of COPPA be updated in order to ensure that the law continues to provide effective safeguards for protecting children's privacy. The online data collection practices of the 1990s have been eclipsed by a new generation of tracking and targeting techniques.[13] We have now entered what many are calling the era of "Big Data," in which the rapid growth of behavioral targeting, including on mobile platforms, along with the integration of online and offline data sources, have created a powerful and ubiquitous digital marketing ecosystem.[14] An entire infrastructure of companies has emerged, specializing in data collection and sales, including demand-side platforms, data exchanges, and data-optimization services. Growing investments in online marketing and data collection companies are expanding the field's capacity to deliver advertising based on the harvesting of an individual users' online data.[15] Vast amounts of user data are now regularly mined and stored in behavioral

---

[12] "Of households with preschoolers, 38% had handheld gaming devices vs. only 24% among those with children aged 6-12. Preschool households also held an edge in laptops (82% to 76%), gaming consoles (76% to 63%) and Internet-capable cellphones (69% to 65%)." Jack Neff, *CyberTots: Pre-teens Drive iPad Purchases, Join Social Networks*, *Advertising Age* (Apr. 20, 2011), http://adage.com/article/news/pre-teens-drive-ipad-purchases-join-social-networks/227101/.

[13] For a detailed description of the latest trends in online behavioral profiling and data collection, see "Comments of the Center for Digital Democracy, et al, In the Matter of A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: Proposed Framework for Business and Policymakers," 18 Feb. 2011, http://www.ftc.gov/os/comments/privacyreportframework/00346-57870.pdf.

[14] *See* Anoop Sahgal, Leveraging 'Big Data': The Next Frontier For CMOs, CMO.com (Sept. 20, 2011), http://www.cmo.com/strategy/leveraging-big-data-next-frontier-cmos?cmpid=TT107.

[15] *See, e.g.*, Devindra Hardawar, "Google acquires Invite Media to Help Users with Ad Exchanges," VentureBeat, 2 June 2010, http://venturebeat.com/2010/06/02/google-acquires-invite-media-to-help-users-with-ad-exchanges/; David Kaplan, "VC Money

targeting warehouses and other databases—and used in an instant to update online targeting profiles. "Data has become one of the most valuable commodities in the real-time bidding system," explained a recent industry report.[16]

Since the initial privacy rules were adopted, the techniques used to track, profile, identify, target, and retarget individuals in the digital environment have become highly sophisticated. Through web analytics, conversation targeting, and other forms of surveillance, marketers can now track individuals online, across media, and in the real world, monitoring their interactions, social relationships, and locations. "Smart" ads stealthily learn about the behavior and interests of individual users in order to deliver personalized advertising messages.[17] Increasingly, behavioral profiles incorporate information from outside databases.[18] New forms of so-called "real-time buying" on advertising exchanges enable consumers—even young ones—to be tracked, profiled, and sold to the highest bidder in milliseconds.[19] The leading online ad companies and agencies, including Google, Yahoo, Microsoft, Omnicom, and WPP, now provide greater use of data captured for online targeting and retargeting of individuals across multiple platforms and services.[20]

Keeps Pouring In For Ad Targeters: Turn Raises $20 Million," paidContent.org, 5 Jan. 2011, http://paidcontent.org/article/419-vc-money-keeps-pouring-in-for-ad-targeters-turn-raises-20-million/ (both viewed 15 Feb. 2011).

[16] Econsultancy, *Demand-Side Platforms Buyer's Guide* 3 (2011), http://econsultancy.com/us/reports/dsps-buyers-guide (purchase required).

[17] *See, e.g.*, Yahoo, "Smart Ads," http://advertising.yahoo.com/article/smart-ads.html. Google's Teracent also provides such ads. Teracent, "Advertiser Solutions," http://www.teracent.com/advertiser-solutions/ (both viewed 23 Dec. 2011).

[18] *See, e.g.*, Experian, "Digital Advertising," http://www.experian.com/business-services/digital-advertising.html; TARGUSinfo, "Our Solutions: On-Demand Verification," http://www.targusinfo.com/solutions/verification/ (both viewed 23 Dec. 2011).

[19] *See generally* AdExchanger.com, http://www.adexchanger.com/; ExchangerWire.com, http://www.exchangewire.com/; Econsultancy, *Online Advertising Survey* (2011), http://econsultancy.com/us/reports/online-advertising-survey (purchase required).

[20] *See, e.g.*, Accuen, "The Trading Desk," http://www.accuenmedia.com/index.htm; Xaxis, "Dazzling Data," http://xaxis.com/; Microsoft Advertising, "Microsoft

The mobile data collection system has also enhanced its capabilities to track and target subscribers by combining behavior, location, and device.[21] Mobile marketing—combining text messaging, mobile video, and other new applications—is one of the fastest growing digital commerce platforms throughout the world.[22] Mobile devices are nearly ubiquitous; smart phones enable access to a rich array of Internet applications, including those taking advantage of GPS; local advertisers have new, inexpensive tools to deliver ads on mobile phones and in stores; and social networks are expanding their enterprises into the mobile arena, through ventures such as FourSquare, Gowalla, and Facebook's own location-based services.[23] Mobile marketers have incorporated behavioral targeting along with location information into their targeting practices.[24] New and emerging data collection techniques, such as "geo-fencing," enable mobile marketers

---

Advertising Exchange," http://advertising.microsoft.com/exchange; Right Media, "The Right Media Exchange," http://rightmedia.com/ (all viewed 23 Dec. 2011).

[21] *See* Yahoo!, "Mobile Internet—Delivering on the Promise of Mobile Advertising," http://advertising.yahoo.com/article/mobile-Internet-delivering-on-promise-of-mobile-advertising.html, Mar. 2011; Phil Mui, "You Can Now See Mobile Ad Performance in Google Analytics," Google Analytics Blog, 11 Nov. 2011, http://analytics.blogspot.com/2011/11/you-can-now-see-mobile-ad-performance.html; Google, "The Mobile Movement: Understanding Smartphone Consumers," YouTube, 13 Apr. 2011, http://www.youtube.com/watch?v=CjUcq_E4I-s&feature=player_embedded#at=16 (all viewed 10 Dec. 2011).

[22] Enid Burns, "U.S. Mobile Ad Revenue to Grow Significantly through 2013," *ClickZ*, 25 Feb. 2009, http://www.clickz.com/3632919 (viewed 23 Dec. 2011).

[23] John Bell, "Brands: Claim Your Facebook Place Today," The Digital Influence Mapping Project, 23 Aug. 2010, http://johnbell.typepad.com/weblog/2010/08/brands-claim-your-facebook-place-today.html (viewed 23 Dec. 2011).

[24] *See* Greg Dowling, "Mobile Measurement," presentation at Engage 2011, http://engage.webtrends.com/blog/category/media-type/presentation/ (viewed 2 Oct. 2011); Dai Pham, "Smartphone User Study Shows Mobile Movement Under Way," Google Mobile Ads Blog, 26 Apr. 2011, http://googlemobileads.blogspot.com/2011/04/smartphone-user-study-shows-mobile.html (viewed 23 Dec. 2011); eMarketer, "Leading Mobile Ad Targeting Tactics According to Advertisers/Agencies in North America," Aug. 2011; Marc Theermann, "Making Mobile RTB Smarter," Google Admeld Blog, 7 Sept. 2011, http://www.admeld.com/blog/view/Making-Mobile-RTB-Smarter/ (viewed 23 Dec. 2011).

to create a "pre-defined, virtual space around a particular location" and know when a child "is within a determined radius."[25]

All of these trends are very much in evidence in the online children's marketplace. For this proceeding we identified how leading children's sites are implementing their online behavioral advertising and digital marketing strategies, drawing from a growing arsenal of powerful data tools to collect "real-time intelligence" from children, which can be used to target them across multiple platforms, including mobile devices, social networks, and interactive games. The following are only a few examples of software and techniques currently in use:

- Disney enables advertisers to target children via "display, video and mobile advertising opportunities." Such ad targeting is available on Disney XD, Disney Junior, Disney Channel, and MarvelKids.com.[26] On its social and gaming platforms, Disney analyzes "large, complex data sets representing the behavior of millions of online social game players."[27] (Disney owns such popular social sites for kids as Club Penguin and Playdom.)[28] Disney uses the Adobe Omniture data profiling system for Disney.com and its other online properties, and employs a wide range of "rich media" and other interactive applications to facilitate its data targeting practices.[29]

---

[25] Placecast, "Shopalerts," http://placecast.net/shopalerts/index.html; *see also* Placecast, "PlaceAd," http://placecast.net/placead/index.html; Navteq Media Solutions, "LocationPoint Advertising," http://navteqmedia.com/mobile/advertising/locationpoint-advertising (all viewed 2 Oct. 2011).

[26] Walt Disney Company, "Disney Media Kit," http://mediakit.go.com/disney/index.html (viewed 23 Dec. 2011).

[27] "'Customer Insight Analyst,' Job in Palo Alto, CA posted by The Walt Disney Company," JobCircle, 17 Dec. 2011 (viewed 23 Dec. 2011).

[28] Leena Rao, "Disney Acquires Social Network For Kids Togetherville," TechCrunch (Feb. 23, 2011), http://techcrunch.com/2011/02/23/disney-acquires-social-network-for-kids-togetherville/; Ben Parr, "Disney Acquires Social Gaming Company Playdom for up to $763.2 Million," Mashable (July 27, 2010), http://mashable.com/2010/07/27/disney-playdom/; Walt Disney Company, "Job Details: Customer Insight Analyst," https://sjobs.brassring.com/1033/ASP/TG/cim_jobdetail.asp?partnerid=25348&siteid=5039&jobid=3143; Walt Disney Company, "Job Details: Account Executive," https://sjobs.brassring.com/1033/ASP/TG/cim_jobdetail.asp?partnerid=25348&siteid=5039&jobid=9147 (all viewed 10 Dec. 2011).

[29] Omniture, "The Walt Disney Internet Group Selects Omniture SiteCatalyst® to Optimize the Customer Experience Across All of Its Online Properties," 13 Sept. 2007,

- Nickelodeon's parent MTV Networks Digital (MTVN Digital) also uses Adobe Omniture's "Online Marketing Suite" to engage in a wide spectrum of web analytics and individual targeting. These include: collecting "actionable viewer data" from a user's "TV, computer, smartphone, or other device," as well as employing "advanced data segmentation" based on data collected from websites, clicks, and other user interactions.[30] Adobe's Test & Target product enables MTVN to assign each individual "a unique visitor ID, which is stored in a cookie on their machine," and used for targeting and behavioral advertising.[31]

- The Cartoon Network's online advertising is facilitated by Turner's Audience and Multi-Platform Technologies group. According to its own award submission for an analytics prize, "Turner is now in the midst of rapidly building out its Audience Insight capabilities—joining Web Analytics with Ad, Mobile and Third Party data… for Ad sales."[32] Among the "advanced targeting" opportunities offered by Turner are "observed interest" ("Based on observed user behavior and content consumption"), "Advanced Retargeting" ("Retargeting based on ad exposure/engagement or based on advertiser data")

---

http://www.omniture.com/press/390 (viewed 10 Dec. 2011). For example, advertisers on Disney can use what's called Rovion InPerson. This "ad opportunity provides the illusion a spokesperson or character is walking across the guest's screen and over site content. . . . The InPerson ad is always positioned so it aligns to the bottom of the screen, above the page fold . . . [, and] the spokesperson or character can be used to promote content or even highlight features on the site for co-branded opportunities." "Manager, Mobile Ad Sales—NYC," Women in Wireless, 21 July 2011, http://womeninwireless.org/manager-mobile-ad-sales-nyc/; Walt Disney Company, "Rovion InPerson," http://mediakit.go.com/disney/richmedia/rovion_InPerson.html (both viewed 10 Dec. 2011).

[30] Adobe TV, "Adobe & MTV Networks," http://tv.adobe.com/watch/customer-stories-web/adobe-mtv-networks/; Adobe, "MTV Networks," http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/customer-success/pdfs/us_91048568_mtvn_ue_fnl_03172011.pdf (both viewed 10 Dec. 2011).

[31] Adobe, "Adobe Test&Target," http://www.omniture.com/en/products/conversion/test-and-target (viewed 10 Dec. 2011); Adobe, "Test&Target—Increase Content Relevance through Conversion Optmization," http://www.omniture.com/en/products/conversion/test-and-target11 (viewed 23 Dec. 2011).

[32] Turner, "SI Digital Sales: CartoonNetwork.com Custom Solutions," http://tsed.turner.com/cartoon-network/custom-solutions/sponsorships; Web Analytics Association, "Innovator/Technology of the Year: Audience Data Best Practices Team, Turner Broadcasting System, Inc," http://www.webanalyticsassociation.org/?page=awards2011_nominees&hhSearchTerms=Turner (both viewed 11 Dec. 2011).

and via "Registration/Contributed Data" ("Zip, Age, Gender targeting—and more").[33]

- Toy manufacturer Mattel is purposefully designing its online properties to enhance and facilitate digital advertising. Its "Mattel Digital Network" (MDN) promises to integrate brands throughout its "prime content," including Barbie.com, HotWheels.com and the new MonsterHigh.com. "[V]eering away from the antiquated ad network model, the new outbound advertising aligns key brands with site-specific content," explains Huge (Mattel's online marketing consultant).[34] Mattel engages in multichannel data analytics to help it achieve "brand and product objectives in the online kids' space."[35]

These practices of extensive data collection run counter to the Fair Information Practice Principles of data minimization, as well as the objectives of the Children's Online Privacy Protection Act and the FTC's current COPPA Rule.

---

[33] Turner, "SI Digital Sales: Audience Segments," http://tsed.turner.com/turner-network/custom-solutions/audience-based-targeting (viewed 11 Dec. 2011). The CN advertising site explains that it is "one of the leading online destinations for Kids 6-11, Boys 6-11, and Tween 9-14…. CartoonNetwork.com's digital offerings are like no other with over 8 million unique visitors per month." The company offers advertisers a range of digital ad applications, including "custom compilations… complete with skins and homepage promotion," "roadblock, content hosting, custom skin," and other "integration" and "takeover" sponsorships. Turner, "SI Digital Sales: CartoonNetwork.com," http://tsed.turner.com/cartoon-network (viewed 11 Dec. 2011). Turner, "Audience & Multi-Platform Technologies," http://ampt.tv/ (viewed 11 Dec. 2011).

[34] Mattel, Mattel Grows Partnership with HUGE (Nov. 18, 2010), http://www.hugeinc.com/news/signed/mattel-audience-monetization; WebGuild, Mattel's *Digital Ad Agency Says Put Advertisers First* (Nov. 22, 2010), http://www.webguild.org/20101122/mattels-digital-ad-agency-says-put-advertisers-first; "Mattel Assoc Manager Digital Marketing in El Segundo, CA," AfterCollege.com, https://www.aftercollege.com/job-channel/gaming-jobs-for-college-students-and-entry-level-job-seekers/42855746/. Mattel is also working with food marketers with its portfolio of games. "Food & Beverage Brands Partner with Mattel Games," MarketWatch, 15 Sept. 2011, http://www.marketwatch.com/story/food-beverage-brands-partner-with-mattel-games-2011-09-15 (all viewed 11 Dec. 2011).

[35] MDN platforms include "online, video game consoles, mobile Interactive TV, and emerging media." Barbie.com, HotWheels.com and the new MonsterHigh.com. "Manager, Global IT, Digital / Web / Multi-Channel Analytics," Dice.com, http://seeker.dice.com/jobsearch/servlet/JobSearch?op=101&dockey=xml/c/4/c4a470ab2baa50740e97893210e01541@endecaindex&c=1&source=34&cmpid=AG:4 (viewed 11 Dec. 2011).

With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled gaming consoles, which are increasingly associated with individual users, rather than families.[36] This means that marketers do not need to know the name, address, or email of a user in order to identify, target, and contact that particular individual.[37]

The entire process of data collection, tracking, and individualized targeting remains opaque and covert, making it virtually impossible for anyone other than the companies themselves to determine exactly how the data are being used to deliver ads to individual children. In preparing these comments, we commissioned two separate studies, which are attached as appendices. The first, by Richard M. Smith of Boston Software Forensics, is included as Appendix A. It surveys the leading websites primarily intended for use by children to understand what Web tracking technologies are employed by the

---

[36] *See* Fed. Trade Comm'n, Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 76 Fed. Reg. 59,804 (Sept. 27, 2011) (citations to the Proposed Rule provided in these comments refer to the page numbers of the version published by the FTC on Sept. 15, 2011) [hereinafter 2011 Proposed Rule] at 35. *See also* Common Sense Media, "Do Smart Phones = Smart Kids?" 21 Apr. 2010, http://www.commonsensemedia.org/about-us/news/press-releases/do-smart-phones-smart-kids (viewed 2 Oct. 2011).

[37] Fed. Trade Comm'n, *Protecting Kids' Privacy Online: Reviewing the COPPA Rule* (June 2, 2010), http://www.ftc.gov/bcp/workshops/coppa/index.shtml (viewed 12 Sept. 2011); Fed. Trade Comm'n Bureau of Consumer Protection, *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 35–38 (Dec. 1, 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. The European Union has also weighed in on this issue, supporting the concept that behavioral targeting information is tied to individuals. Data Protection Working Party, "Opinion 2/2010 on Online Behavioural Advertising, 22 June 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (all viewed 13 Sept. 2011). See also Wendy Davis, "ClearSight Launches Targeting Platform Tying IP Addresses To Offline Data," *Online Media Daily*, 28 June 2010, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=131044 (viewed 2 Oct. 2011).

sites. The second, by privacy attorney Sharon Goott Nissim, is included as Appendix B. This study examines the privacy policies of the most popular children's websites to discern patterns of information practices and policies, and to determine whether or not popular children's website operators are complying with the current version of the COPPA Rule.

For each study, the Rudd Center for Food Policy & Obesity at Yale, in collaboration with the Center for Digital Democracy and the Institute for Public Representation, provided the researchers with a list of top children's websites. These websites were selected based on data provided by comScore. comScore captures the Internet behavior of a representative panel of about 1 million users in the United States.[38] It is the nation's largest existing Internet audience measurement panel. The firm collects data at both the household and individual level using Session Assignment Technology, which can identify computer users without requiring them to log in. The company uses these panel data to extrapolate its findings to the total U.S. population. Using the comScore panel, we identified the 50 websites defined by comScore that contained Kids Entertainment content (activities, online games, etc.) that had the highest average number of visitors ages 2–11 years during July, August, and September of 2011. These data are from the comScore Media Metrix Key Measures Report.[39] The Media Metrix database provides Internet exposure data for any websites visited by at least 30 of their panel members in a given quarter.[40] Media Metrix also provides exposure information by visitor age for larger volume websites.

---

[38] comScore, U.S. Client Newsletter, Aug. 2009, www.comscore.com/Newsletter/2009/August/US_Client_Newsletter (viewed 10 Dec. 2011).

[39] comScore, Media Metrix Core Reports, 2011, comscore.com/Products_Services/Product_Index/Media_Metrix_Suite/Media_Metrix_Core_Reports (viewed 2 Oct. 2011).

[40] comScore, U.S. Client Newsletter.

Our findings raise a number of concerns that we urge the Commission to address in its final deliberations on the proposed rules. An overwhelming 81% of the top children-oriented websites analyzed were found to employ some form of tracking and/or targeting. Almost half (48%) are engaging in behavioral ad targeting. Based on what we have found, it is clear that sites directed at children use a wide range of persistent identifiers to track behaviors of children interacting with sites.

The FTC's proposed rule changes would help address some of these practices, requiring operators of child-oriented online services who use IP addresses or other persistent identifiers for purposes other than to support the internal operations of a website to first obtain parental consent. Although this would not affect operators who use persistent identifiers only to conduct normal business operations (including those who serve contextual advertisements), it would create safeguards when the identifiers are used to behaviorally target an individual child, create a profile based on that child's online activities, or share the information with third parties.[41] While recognizing the technological changes and prevailing business practices that have eroded anonymity on the Internet, the Commission has proposed a very narrow and careful policy for bringing the COPPA Rule up to date.

There is considerable evidence in the scientific literature on child development, and on children's responses to advertising, to raise serious questions about the fairness of the contemporary techniques marketers use to target young people online.[42] "Because

[41] Fed. Trade Comm'n, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule," 15 Sept. 2011, http://www.ftc.gov/opa/2011/09/coppa.shtm (viewed 2 Oct. 2011).

[42] Dale Kunkel and Jessica Castonguay, "Children and Advertising: Content, Comprehension, and Consequences," in Dorothy G. Singer and Jerome L. Singer, Eds., *Handbook of Children and the Media,* Second Edition. Sage Publications: 2012; Louis J. Moses, "Research on Child Development: Implications for How Children Understand and Cope with Digital Media," Memo prepared for the Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children for the NPLAN Marketing to Children Learning Community, Berkeley, CA, June 29-30, 2009, http://www.digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (viewed 26

young children lack the cognitive skills and abilities of older children," explains an authoritative report from the American Psychological Association, "they do not comprehend commercial messages in the same way as do more mature audiences, and hence, are uniquely susceptible to advertising influence."[43] Such vulnerabilities are further exacerbated in digital media. The growth of online video, interactive games, and virtual worlds means that children are not just *viewing content,* but *inhabiting media environments* where entertainment, communication, and marketing are combined in a seamless stream of compelling sounds and images. Because digital marketing routinely blurs the lines between content and advertising, children have greater difficulty even discerning the commercial content in online environments.[44] Children's attention online "may be largely engaged with the interactive experience," explains child development scholar Louis Moses. As a consequence, their ability to attend consciously to the marketing techniques "may be processed only peripherally, and thereby less deeply."[45] Even in cases where children recognize that marketers are trying to influence them, they may be thwarted in their understanding because of the powerful nature of digital

---

Aug. 2010); Xiaomei Cai and Xiaoquan Zhao, "Click Here, Kids! Online Advertising Practices on Popular Children's Websites," *Journal of Chlidren and Media,* Vol. 4. No. 2, 2010. D. Roedder-John, "Consumer Socialization of Children: A Retrospective Look at Twenty-five Years of Research," *Journal of Consumer Research* 26, n. 3 (1999): 183-213.

[43] Dale Kunkel, Brian L. Wilcox, Joanne Cantor, et al., "Report of the APA Task Force on Advertising and Children," 20 Feb. 2004, http://www.apa.org/releases/childrenads.pdf, p. 1.

[44] Dale Kunkel and Jessica Castonguay, "Children and Advertising: Content, Comprehension, and Consequences"; M. Ali, M. Blades, M. C. Oates, and F. Blumberg, "Young Children's Ability to Recognize Advertisements in Web Page Designs," *British Journal of Developmental Psychology.* Vol. 27, No. 1. Pp. 71-83; M. McIlrath, "Children's Cognitiive Processing of Internet Advertising," Unpublished Doctoral Dissertation, University of California, Santa Barbara. http://dl.acm.org/citation.cfm?id=1269502 (viewed December 22, 2011).

[45] Moses, *supra* note 42.

marketing environments, which are often "interactive, immersive, alluring, engaging, and motivationally and emotionally rewarding."[46]

The online industry's own research has documented children's inability to process some of the prevailing techniques used in contemporary digital marketing. For example, a recent usability study of children's websites found that children often "mistake promotional content for real content, and thus can be distracted away from a website and are more vulnerable to commercial promotions."[47] Some children's sites appear to be taking advantage of these cognitive limitations in designing children's online content and services. The report cites an example from the Cartoon Network website, where, "when children clicked on a game, they were shown an ad while the game was loading. Sometimes the ad was static, and sometimes it was interactive. When it was interactive, it often contained invitations to "Play now" or links to a different page. Kids could easily confuse the "Play now" in the ad with an invitation to start the game they had actually chosen."[48]

Because of the ubiquity of digital media, marketing is now woven into the very fabric of young people's daily experiences, following them wherever they go on a 24/7 basis. Today's techniques for tracking, profiling and behavioral targeting enable marketers to follow children's movements and behaviors from moment to moment, assessing their reactions to various advertising and sales appeals. As a result, marketing messages can be tested, refined, and tailored for maximum effect.[49]

---

[46] Moses, *supra* note 42.
[47] Raluca Budiu and Jakob Nielsen, "Usability of Websites for Children: Design Guidelines for Targeting Users Aged 3–12 Years," 2nd edition, 2010, http://www.nngroup.com/reports/kids/ (purchase required). P. 34.
[48] Raluca Budiu and Jakob Nielsen, "Usability of Websites for Children: Design Guidelines for Targeting Users Aged 3–12 Years," p. 223.
[49] See Kathryn Montgomery, Sonya Grier, Jeff Chester, and Lori Dorfman, *Food Marketing in the Digital Age: A Conceptual Framework and Agenda for Research*, Apr. 2011, http://digitalads.org/reports.php (viewed 2 Oct. 2011).

Given children's limited cognitive abilities and the sophisticated nature of contemporary digital marketing and data collection, strong arguments can be made that behavioral targeting is an inappropriate, unfair, and deceptive practice when used to influence children under 13. At the very least, marketers should be constrained from engaging in such practices without obtaining meaningful, prior consent from parents. This is the mechanism created under the COPPA framework, and we have argued in our comments that the Commission must ensure parents are fully informed of the nature and extent of data collection before making any decisions about how marketers can interact with their children. However, our research on children's online privacy policies, described below, demonstrates that current disclosure practices are too often incomplete, inaccurate, and confusing.

To discern patterns of information practices and policies, and to determine whether or not children's website operators comply with the current version of the COPPA Rule, CDD asked an independent consumer privacy expert to examine over 50 privacy policies of top child-oriented websites. From our research we determined that while many children's websites are fully engaged in tracking, profiling, and behavioral targeting, operators are not doing a good job of informing parents of the practices. What they promise advertisers is in stark contrast to what they tell parents about their data collection practices. At best, these companies are providing less than adequate disclosure of their privacy practices. At worst, they fail to meet even the minimum standards for notice required under the COPPA Rule. Moreover, third parties that routinely collect information from children on these sites and target them are not revealed and do not display any privacy policies to explain their practices. Parents have no way of knowing that these companies are engaging with their children and tracking their behaviors. These patterns are woefully inconsistent with COPPA's intent.

For example, Turn's data collection and targeting services are, according to Forrester "for big, analytically minded buyers looking for a scaled solution to integrated

audience data management and media buying and optimization."[50] Through a combination of ad network and ad exchange services, Turn integrates nearly a dozen other data "partners" to promote individualized advertising in "real-time."[51] They include AdAdvisor/TARGUSinfo, Brilig, Blue Kai and others.[52] Turn has helped Experian transform "de-identified offline data representing an audience of 400 million into actionable insights for the targeting of online display ads."[53] According to the research commissioned by CDD in connection with these comments, Turn is operating on Webkinz World,[54] a website "designed for users aged 6-13+."[55] However, the privacy policy for Webkinz World does not disclose Turn's practices, instead disclaiming any responsibility for the "tracking technologies" of "third-party advertising service providers."[56] The privacy policy directs interested parents to the Network Advertising Initiative (NAI) for more information about the information collection practices of advertising partners, but Turn is not even a member of NAI.[57]

Contemporary advertising practices—including widespread tracking, individualized targeting, location-based information collection, rapid mobile market growth, and improved facial recognition techniques—highlight the necessity for the FTC to update the COPPA Rule. By choosing to do so now, the Commission has taken a timely, responsible, inclusive, and thoughtful approach to its responsibility for ensuring the law's continued effectiveness, enlisting the input of a wide range of experts and stakeholders in a series of workshops, discussions, and written comments over the past

---

[50] http://www.marketwatch.com/story/dataxu-named-a-demand-side-platform-leader-and-ranked-number-one-in-current-offering-by-independent-research-firm-2011-12-14.
[51] http://www.turn.com.
[52] http://www.turn.com/?page_id=8255.
[53] http://www.turn.com/?p=7147.
[54] Appendix A at 11.
[55] Webkinz, For Parents – FAQ: How Does this Site Appeal to Small Children?, http://www.webkinz.com/us_en/faq_parents.html (last visited Dec. 22, 2011).
[56] Ganz, Webkinz – General Privacy Policy, http://www.webkinz.com/us_en/privacy_policy.html (last visited Dec. 22, 2011).
[57] *See* http://networkadvertising.org/participating/.

several years. The proposed revisions to the Rule offer a sensible set of recommendations, reflecting the interests and concerns of the many participants involved in the Commission's widespread consultation efforts. We believe these changes will help address a number of problems raised by consumer groups, privacy experts, and child advocates.[58]

II. Children's Privacy Advocates Generally Support the Proposals to Clarify and Update the Definitions in the COPPA Rule

COPPA generally prohibits any website or online service directed to children or that has actual knowledge that it is collecting information from a child, to collect information without providing adequate notice to and obtaining verifiable parental consent from parents prior to the collection, use, or disclosure of personal information from children. COPPA further delegates authority to the FTC to promulgate rules to implement COPPA and to periodically review those rules. The definitions section of the COPPA Rule is crucial to COPPA's effectiveness.

A. Overview of Proposed Changes

The FTC has proposed a set of modifications to the definitions that are intended to work together to better protect children's privacy, while at the same time encouraging the continuing growth of engaging, diverse and appropriate online content for children. The terms that the FTC proposes to clarify or modify are: "collects, or collection," "disclosure," "release of personal information," "support for internal operations," "online contact information" and "personal information." CCD et al. strongly support most of these proposals.

---

[58] Fed. Trade Comm'n, FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule (Sept. 15, 2011) http://www.ftc.gov/opa/2011/09/coppa.shtm.

1. Definitions of "Personal Information" and "Support for Internal Operations"

The most significant proposal is to expand the definition of "personal information" to account for new technologies and marketing practices. Specifically, the FTC proposes that personal information would include a "persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the website or online service." It is important to note that while this definition expands the definition of personal information, it also provides an important limitation—it will allow operators to use persistent identifiers for "internal operations."

The FTC also proposes to add an identifier that links the activities of a child across different websites or online services. This addition is intended as a "catch-all category covering the online gathering of information about a child over time for the purposes of either online profiling or delivering behavioral advertising to that child."[59] It would cover, for example, an advertising network that tracks a child across website but store the information in a separate database. Children's Privacy Advocates support this proposal as well. Taken together, revised sections (g) and (h) should effectively prevent the use of children's data for behavioral advertising without informed and affirmative parental consent, but would allow this data to be used for activities necessary to maintain the technical functioning of the website or online service.

The FTC also proposes to include within the definition of personal information:

- Screen or user names when they are used for functions other than support for the internal operations;

[59] 2011 Proposed Rule, *supra* note 36, at 37–38.

- A photograph, video, or audio file where such file contains a child's image or voice; and
- Geolocation information sufficient to identify street name and name of a city or town.

Children's Privacy Advocates support these changes for the reasons explained below. The FTC also seeks comment on whether to include ZIP+4 or the combination of date of birth, gender and ZIP code in the definition of personal information.[60] We support including these in the definition of personal information.

2. Definition of "Collects or Collection"

Children's Privacy Advocates also support the change in the definition of "collects or collection" to clarify that it covers online collection whenever an operator mandates, prompts or encourages a child to provide personal information.[61] Children's Privacy Advocates also support the simplifying the language to clarify that all means of passive tracking are considered collection.[62] But Children's Privacy Advocates are concerned about the proposal to replace the current interpretation of "collects or collection," that allows children to publicly post personal information on social networking sites only where the operator deletes all personally identifiable information before the postings are made public and deletes this information from its records, with a "reasonable measures" standard.[63] While we support the purpose of this exception, we are concerned that there is insufficient research demonstrating that the automated filtering techniques that would be allowed under the reasonable measures standard would be effective.[64]

---

[60] 2011 Proposed Rule, *supra* note 36, at 43.
[61] 2011 Proposed Rule, *supra* note 36, at 19.
[62] *Id.* at 22.
[63] *Id.* at 19.
[64] Children's Privacy Advocates also support the proposed clarification that "online contact information" term includes *but is not limited to* commonly-used online identifiers such as IM, VoIP and chat user identifiers. *Id*. at 28.

B. Persistent Identifiers Must Be Included in the Definition of Personal Information

COPPA directs the FTC to adopt regulations prohibiting unfair and deceptive acts and practices in connection with the collection and use of personal information from and about the Internet.[65] In 2009, the FTC issued a report and recommended guidelines for behavioral advertising, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*. The self-regulatory principles, which were the subject of extensive public comment, state that companies should obtain express affirmative consent before collecting sensitive information for behavioral advertising purposes.[66] The Commission considers information about children one of the "clearest examples" of sensitive data.[67] When the guidelines were published, then-Commissioner Leibowitz explained that extra protection is warranted for children's information because that data is "so sensitive" and children are "so vulnerable."[68] Children's Privacy Advocates agree. And we note that some industry voluntary guidelines also prohibit behavioral targeting of children.[69]

---

[65] § 1303.
[66] *Id*. at 47.
[67] Data about health or finances were the other named clear examples of sensitive information
[68] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (Feb. 2009) (Comm'r Jon Leibowitz, Chairman, Fed. Trade Comm'n, concurring), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf. Lydia Parnes, the former director of the Commission's Consumer Protection Bureau, also testified before Congress that consumer tracking concerns are exacerbated when the tracking involves sensitive information about children. Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (July 9, 2008) (prepared statement of the FTC), available at http://www.ftc.gov/os/2008/07/P085400behavioralad.pdf.
[69] *See, e.g.*, Self-Regulatory Principles for Online Advertising at 16, *available at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf (Section VI, Sensitive Data, states that "Entities should 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*

Nonetheless, a survey of the fifty most popular children's websites by the *Wall Street Journal* in 2010 "found that popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults."[70] In the NPRM, the Commission recognizes that "it is unclear from the record before the Commission whether operators currently are directing online behavioral advertising to children." It notes that "various members of industry have informed Commission staff that they do not believe such activity is occurring while media reports have indicated the widespread presence of tracking tools on children's websites."[71]

1. New Research Reveals Widespread Tracking and Behavioral Advertising on Websites Most Popular with Children

To determine the amount of online behavioral advertising to children being conducted currently, CDD asked Richard M. Smith of Boston Software Forensics to survey tracking and targeting techniques employed on 54 leading child-targeted websites.[72] Smith found that most (81%) engage in some form of tracking and/or targeting:

---

directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA." (emphasis added)).

[70] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, Wall Street J. (Sept. 17, 2010), http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html.

[71] 2011 Proposed Rule, *supra* note 36, at 39, n. 86.

[72] Using the comScore panel, we identified the 50 websites defined by comScore that contained Kids Entertainment content (activities, online games, etc.) that had the highest average number of visitors ages 2–11 years during July, August, and September of 2011. We then provided Smith with a suggested dataset that included the privacy policy of at least one website from each top company that operates at least one site with a non-foreign top-level domain, as well as a few of the most popular websites owned by top companies that operate . For companies in control of several child-oriented websites, the privacy policies of multiple sites were examined and, if found to differ materially from each other, the sites were included separately in the dataset. The privacy policies examined for this report are meant to closely approximate, but not exhaustively comprise, the privacy policies of the 50 child-targeted companies most popular among U.S. children online.

Tracking technology	Web site count	Percentage
First-party cookies	44	81%
Internet ad network tracking	38	70%
Behavioral ad targeting	26	48%
Web analytics	45	83%
Registration data	23	42%

Almost half (48%) are engaging in behavioral ad targeting and many use more than one type of tracking and/or targeting.

2. Operators Employ Methods of Tracking and Behavioral Advertising on Children's Websites

Smith explains how behavioral advertising works. The components include cookies, web bugs, flash cookies, registration data, and IP addresses.

Cookies are the foundation for web tracking. Smith analogizes them to membership cards:

> The first time someone visits a Web site, they are given a membership card for the Web site in the form of a cookie. The membership number on the card is the unique ID number of the cookie. The membership card and number are stored away on the user's hard drive. Each time a person returns to the Web site, their membership card number is sent back to the Web site, allowing the Web site to track what a person has been doing at the Web site over time.[73]

Smith further explains that "because of the underlying architecture of the Web, the components of a Web page can come from many different Web servers run by multiple vendors." For example, Smith examined the most visited children's website, nick.com, and found that its home page contained more than 250 requests for components from about 25 different web servers. Some of the servers are run not by Nick.com but by third-party vendors such as Internet ad networks, content delivery networks for multimedia files, and web analytics companies. Smith explains:

[73] Appendix A at 8.

> Just like a Web site itself, a third-party vendor can use cookies when a browser makes a request for a Web page component to its servers. . . .
>
> For example, nick.com uses the DoubleClick ad network to show banner ads at the nick.com Web site.
>
> . . . .
>
> Using the membership analogy . . . , when a child visits the nick.com Web site, they quietly become members of both the nick.com Web site and the DoubleClick ad network.
>
> When visiting the nick.com Web site with all cookies cleared out from a browser, at least 6 cookies are set by different vendors, all which appear to contain unique tracking id numbers in them.
>
> When a Web page component is being fetched from a third-party server, a browser will also send the URL of the Web page that the component is part of to the server as part of the request for the component. This URL is sent as a header line in the request and is known as the referring URL or referrer.
>
> Using the referring URL, an Internet ad network can then keep track of the Web pages that someone visits and use this information for ad targeting purposes. However, unlike a single Web site that only gets to track click-stream data on their own Web site, an Internet ad network can do tracking of individuals across many different Web sites that are part of the ad network. This multi-site tracking ability provides more even more data to develop profiles of individuals for ad targeting purposes.[74]

Smith also describes a related tracking technology called a "web bug." Web bugs are also known as web beacons, clear pixels, and tracking pixels. They are invisible to website visitors. Web bugs can be used to collect data to create aggregate statistics about website usage. The collection of aggregate statistics is known in the industry as web analytics.

Internet ad networks also use Web bugs to collect data for ad tracking purposes. Smith explains that this "second use of Web bugs targets individual visitors to a Web site as opposed to looking at group behavior as is done with Web analytics."[75] Although

[74] *Id.* at 8–9.
[75] *Id.* at 10.

third-party tracking technologies are typically invisible to a person visiting a website, there are a number of browser tools that show when these technologies are being employed at a website. Using one such tool, Smith found five web bugs on the nick.com home page, that provide data to comScore, Crazy Egg, DoubleClick, Google, and Quantcast.[76] These companies can use this data for behavioral advertising. Quantcast, for example, claims it can "[s]egment out specific audiences you want to sell across your content. Adjust the composition of your audiences to index higher and target audiences that were previously challenging to deliver."[77]

Smith also found that Nick.com passes data that children provide when registering to Adobe's Demdex.[78] According to Demdex's website, Demdex "empower[s] your company to create a 'Data Bank' of audiences with data captured from your web properties, purchased from third-party data sellers or exchanges, and generated from your ad campaigns."[79] Nor is Nickelodeon the only child-directed company that works with behavioral ad targeting services. Disney's website, for example, shares information with AudienceScience, which claims to be "the largest and most trusted audience aggregator in the world."[80]

Ganz[81] and others work with TARGUSinfo, a company that openly boasts the ability to achieve "online/offline fusion"—in other words, the ability to match online user data with information about their offline life. TARGUSinfo claims it can extract information about users from "verified, household-level offline consumer demographics" including "family status, number of children, hobbies, home ownership, lifestyle patterns, hobbies and avocations, discretionary purchase priorities, brand and product affinities,

---

[76] *Id.*
[77] *Id.* at 5 (*citing* http://www.quantcast.com/audience/reach-audience-for-media-sellers).
[78] *Id.* at 19.
[79] http://www.demdex.com.
[80] Appendix A at 3; http://www.audiencescience.com/technology.
[81] Ganz is the subject of a recent complaint and request for investigation filed with the FTC by the Campaign for a Commercial-Free Childhood.

education, income and occupational status."[82] TARGUSinfo is able to extract these highly personal details about an individual user using only the information provided by one its online partners.[83]

Many child-oriented websites work with multiple behavioral ad targeting services. On the Webkinz home page alone, Smith found thirteen tracking tools belonging to nine advertising service providers.[84]

Smith notes that many websites ask children to provide demographic data at registration. For example, the sign-up page for Nick.com asks children for a "nickname," birthday (month, day and year), and gender. The sign on page tells kids that collecting birthdays "helps us make new stuff just for you, which helps make Nick.com even better!" It states that it asks for gender "so we can make Nick.com the best it can be for ALL of our fans." But Smith points out that "[o]nce this information is submitted to nick.com, it will be associated with the nick.com cookie in a database at nick.com. Later on the information can be used for ad targeting purposes at the nick.com Web site and potential other Web sites."[85]

Smith analogizes IP addresses to phone numbers. "An IP address identifies a computer on the Internet in much the same way that a phone number indentified a phone on the phone network."[86] He explains that IP addresses are used for many types of tracking, including approximate geographic location.[87]

Smith describes how behavioral advertising works:

---

[82] TARGUSinfo, *Taking Online Targeting to the Next Level* 10 (2009), http://www.targusinfo.com/files/PDF/white_papers/TakingOnlineTargetingtotheNextLevelWhitepaper.pdf.
[83] *Id.*
[84] Appendix A at 11.The companies and tools encountered were: Acerno, Adnetik, Casale Media, Google (DoubleClick, DoubleVerify, DoubleVerify Notice, Google Adsense, and Google Analytics), MediaMath, Microsoft Atlas, Nielsen (NetRatings SiteCensus), Quantcast, and Turn.
[85] Appendix A at 13.
[86] *Id.* at 13.
[87] *Id.* at 14.

> Behavioral targeting is based on building a profile for each visitor to a Web site. The data of a profile are typically stored in a database belonging to a Web site, Internet advertising network, or a vendor who specializes in behavioral tracking. A profile is created for a visitor the first time they come a Web site. The profile is identified by an id number stored in a browser cookie.
>
> . . . .
>
> The following sources of data are used to construct a visitor profile over time:
>
> - The URLs of the click-stream for the visitor, which indicate the type of content that the visitor is interested in
> - The IP address of the visitor
> - Registration data supplied by the visitor
> - Searches done by a visitor at a Web site
> - Data from other Web sites that are collected by an ad network or a behavioral tracking company
>
> From this data, a Web site can use data mining techniques to draw inferences about a particular person using the Web site.[88]

3. The Inclusion of Persistent Identifiers Is Necessary to Protect Children

When the FTC adopted the initial COPPA Rule in 1999, it declined to include IP addresses as personal information unless they were associated with other individually identifiable personal information. Now, the FTC has re-examined this decision in light of developments over the past twelve years and concluded that "persistent identifiers can permit the contacting of a specific individual," and should be included, with some limitations, within the definition of "personal information" in the COPPA Rule.[89] The Commission correctly rejects claims that that persistent identifiers only allow operators to contact a specific device or computer, finding that,

> Information that 'permits the physical or online contacting of a specific individual' does not mean information that permits the contacting of only a single individual, to the

[88] Appendix A at 16.
[89] 2011 Proposed Rule, *supra* note 36, at 34.

> exclusion of all other individuals. For example, the COPPA statute includes within the definition of 'personal information' a home address alone or a phone number alone—information that is often applicable to an entire household.[90]

Smith's analogies of cookies to membership cards and IP addresses to telephone numbers show why the Commission's position is correct. Just as in 1999, home addresses, telephone numbers, and email addresses were all considered personal information, so should cookies, IP addresses, and the like be considered personal information today.

Children's Privacy Advocates also agree with the FTC that there has been a shift from the family computer or device to the personal computer or smart phone.[91] Children are no exception to this trend as they increasingly have access to the Internet through personal mobile devices at younger and younger ages.

Children's Privacy Advocates believe that the FTC's decision to include persistent identifiers under the definition of personal information will not inhibit operators' use of contextual advertising, a commonly accepted practice that is distinct from behavioral advertising and its concomitant privacy concerns. Operators that rely on advertising to monetize their sites and online services need not engage in *behavioral* advertising as a source of revenue. As the Commission explained in its proposed privacy framework, "Contextual advertising involves the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection

---

[90] *Id.* at 38–39.

[91] 2011 Proposed Rule, *supra* note 36, at 35. *See also* Roger Entner, *Under-Aged Texting Usage and Actual Cost,* Nielson Wire, Jan. 27, 2010, http://blog.nielsen.com/nielsenwire/online_mobile/under-aged-texting-usage-and-actual-cost/; Ethan Lyon, *Examining Generation Z: Stats, Demographics, Segments, Predictions*, Sparxoo: Branding Experts for the Digital Era, Feb. 23, 2010, http://sparxoo.com/2010/02/23/examining-generation-z-stats-demographics-segments-predictions/; Dan Frommer & Kamelia Angelova, *One Third of U.S. 11-Year-Olds Have Cellphones*, Business Insider, (Jan. 2010) *available at* http://articles.businessinsider.com/2010-01-19/tech/30037917_1_cellphones-mobile-phones-content.

and retention of data about the consumer's online activities over time" and thus "presents minimal privacy intrusion as compared to other forms of online advertising" like behavioral advertising.[92] Further, the notion that tracking is the only way to advertise today is false because a thriving online environment supported by advertisements existed before behavioral advertising became widely adopted.[93]

Thus, Children's Privacy Advocates support the Commission's proposal to add to the definition of "personal information" a revised section (g) and a new section (h). The effect of this change will be to put an end to the extensive tracking and behavioral targeting of children already occurring without the knowledge and consent of parents, while allowing persistent identifiers to be used to support the internal operations of the website or online service.

C. Personal Information Should Include Screen and User Names

Currently, screen names are only considered personal information if they reveal an individual's email address. The Commission proposes that because screen names permit the direct contact of a specific individual online regardless of whether they contain an email address, screen or user names should be categorized as personal information whenever they are used for functions other than or in addition to support for internal operations.[94] Children's Privacy Advocates support this proposal.

There is no question that the operator of a website or online service can use screen or user names to directly contact individuals online. Moreover, it is also possible for third parties to identify and contact individuals if they know the user name. People commonly use the same screen names for accessing different websites for ease in remembering login

---

[92] FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change, (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[93] Jonathan Mayer, *Do Not Track Is No Threat to Ad-Supported Businesses,* Stanford Center for Internet and Society (Jan. 20, 2011), http://cyberlaw.stanford.edu/node/6592.

[94] 2011 Proposed Rule, *supra* note 36, at 30.

information. Reused screen names can be used to link a user's activities across different sites, as well as lead to the discovery of extensive data associated with the user.[95] As a result, "a username is likely sufficient to link accounts across websites."[96] After a link is made between separate accounts, data across the accounts can be used to identify an individual.[97]

A recent research paper, *How Unique and Traceable are Usernames?* found that "it is possible, with high precision, to link accounts solely based on usernames. This is due to the high average entropy of usernames and the fact that uses tend to choose usernames that are related to each other."[98] This paper further concluded that it is "clearly possible to tie digital identities together and, most likely, to real identities in many cases *only* using ubiquitous usernames."[99] This can be accomplished with "high accuracy and minimum effort," without the user ever giving consent.[100] The data set or profile created from the user's different accounts "often provides a sufficiently comprehensive mosaic to identify an individual."[101] Thus, screen and user names should be included in the definition of personal information, as the FTC has recommended.

D. Personal Information Should Include Geolocation Information

The Commission notes that geolocation services have become "ubiquitous features of the personal electronics market."[102] The Commission further states that geolocation information sufficient to identify the name of a street and city or town is

---

[95] *See* Jonathan Mayer, *Where Everybody Knows Your Username*, The Center For Internet and Society (Oct. 11, 2011), http://cyberlaw.stanford.edu/node/6740.
[96] *Id.*
[97] *Id.*
[98] Daniele Perito, Claude Castelluccia, Mohamed Ali Kaafar, & Pere Manils, *How Unique and Traceable are Usernames?, available at* http://planete.inrialpes.fr/papers/high_entropy.pdf, at 14.
[99] *Id.* (emphasis added).
[100] *Id.*
[101] Mayer, *supra* note 95.
[102] 2011 Proposed Rule, *supra* note 36, at 41.

already covered under COPPA Rule 312.2's category covering a "home or other physical address including street name and name of a city or town." However, to clarify its rules, it proposes to add a separate section specifically addressing geolocation information.

Children's Privacy Advocates support this proposal. Children are avid uses of mobile devices. A recent study by Ipsos, based on online interviews of 2,080 children and 715 parents demographically and geographically representative of the U.S. between January 31 and February 14, 2011, found that half of eleven-year-olds have their own mobile phones.[103]

The Ipsos study also found that "[p]re-teen and even pre-school children are key drivers for adoption of the iPad and other tablet computers." It found that 10% of households with children aged 6–12 and pre-schoolers have iPads, compared to 3% of households without pre-teen children and that 27% of households with kids aged 6–12 plan to purchase an iPad and 35% some brand of tablet computer in the next year.[104] Other surveys have made similar findings. For the second year in a row, the Apple iPad is the "most desired consumer electronic among kids ages 6–12" this holiday season.[105]

While children today already use mobile devices, the Ipsos study suggests that children are using mobile devices at younger ages. According to the study, "pre-schoolers are adopting digital habits or being exposed to new devices even faster than tweens, a

---

[103] Jack Neff, *CyberTots: Pre-Teens Drive iPad Purchases, Join Social Networks,* Advertising Age (Apr. 20, 2011) http://adage.com/article/news/pre-teens-drive-ipad-purchases-join-social-networks/227101/.

[104] *Id.; see also Adam Satariano and Katie Linsell, IPad-Crazed Toddlers Spur Holiday Sales, Bloomberg (Nov. 28, 2011),* http://www.bloomberg.com/news/2011-11-28/apple-s-digital-pacifier-ipad-has-parents-emptying-their-wallets-tech.html *(*"According to Forrester Research Inc. (FORR), 29 percent of tablet owners regularly share the device with their kids. Among mothers, it's 65 percent. One Apple commercial shows a young child learning to write using the iPad 2.").

[105] *U.S. Kids Looking Forward to "iHoliday" 2011*, NielsenWire (Nov. 17, 2011), http://blog.nielsen.com/nielsenwire/consumer/us-kids-looking-forward-to-iholiday-2011/. Nearly half of kids have expressed interest in an iPad this year, up from 31% in 2010. The iPod Touch and iPhone "round out kids' top three."

sign of the speed with which digital technology is reshaping media and marketing habits for the youngest children."[106] Donna Sabino, a senior vice president for Ipsos OTX, explains, "If you're a digital native parent and have a smartphone that accesses the Internet and gets apps, it's not out of the realm of possibility for you to introduce your child to that when they're 1, 2 or 3."[107]

The wide availability of mobile and geolocation devices and services can provide marketers and others with easy access to information about children's online behavior and physical location. "Profiling of mobile customers makes it possible for advertisers to generate ads that are more personalized (individualized) and more localized (location-specific) as compared to traditional online behavioural advertising."[108]

Mobile apps, which often facilitate the collection of information from users, are increasingly being marketed explicitly to children.[109] Kids Industries, a London marketing company that specializes in children and families, reveals that "pester power [is] the main incentive for downloads" of mobile apps, with over 40% of parents surveyed stating that they downloaded an app to satisfy their child's request for that app.[110]

Information about the location of a child is especially sensitive because it can allow for a child to be physically contacted wherever he or she is. The risks of using such services can be magnified for children, who often fail to comprehend the significance of

---

[106] Neff, *supra* note 103.
[107] Neff, *supra* note 103.
[108] Nancy J. King & Pernille Wegener Jessen, *Profiling the Mobile Customer – Privacy Concerns When Behavioural Advertisers Target Mobile Phones – Part I*, 26 Computer Law & Security Review 455, 461 (2010).
[109] *See, e.g.*, Tamsin Oxford, *10 best free Android apps for kids*, techradar.com (May 17), http://www.techradar.com/news/mobile-computing/tablets/10-best-free-android-apps-for-kids-956171; Sam Cater, *30 Android Applications for Children* (June 23, 2011), http://android.appstorm.net/roundups/entertainment/30-android-applications-for-children/.
[110] Gary Pope, Kids Industries, *Apps 2011* 5, *available at* http://blog.kidsindustries.com/2011/10/kids-apps-report-up-for-download/.

sharing information. For all of these reasons, it is important that no geo-location information be collected from children without affirmative and informed parental consent.

E. Personal Information Should Include Photographs, Videos, and Audio Files

The Commission proposes to include within the definition of personal information "a photograph, video, or audio file where such file contains a child's image or voice."[111] The Commission explains that photos can be very personal in nature and can be identified using facial recognition techniques or other methods.

Children's Privacy Advocates support this proposal. The use of facial recognition technology is rapidly increasing, raising privacy concerns for Internet users of all ages.[112] For example, a recent study by researchers at Carnegie Mellon found that it "is possible to identify strangers and gain their personal information—perhaps even their social security numbers—by using face recognition software and social media profiles."[113]

---

[111] 2011 Proposed Rule, *supra* note 36, at 41.

[112] Natasha Singer, *Face Recognition Moves from Sci-Fi to Social Media,* N.Y. Times (Nov. 12, 2011), *available at* http://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.html?_r=3&ref=technology; Shauna Wright, *Facial Recognition Software Now Being Used for Personalized Marketing,* News Radio 1310 KLIK (Nov. 2011) *available at* http://newsradio1310.com/facial-recognition-software/; Sarah Jacobsson Purewal, *Why Facebook's Facial Recognition is Creepy,* PC World (Jun. 11, 2011) *available at* http://www.pcworld.com/article/229742/why_facebooks_facial_recognition_is_creepy.html; Jennifer Valentino-DeVries, Tech Today: Using Facebook and Facial Recognition to ID Random People, The Wall Street Journal, Aug. 1, 2011, http://blogs.wsj.com/digits/2011/08/01/tech-today-using-facebook-and-facial-recognition-to-id-random-people/

[113] Carnegie Mellon University, Press Release: Face Recognition Software, Social Media Sites Increase Privacy Risks, Says New Carnegie Mellon Study (Aug. 1, 2010) http://www.cmu.edu/news/stories/archives/2011/august/aug1_privacyrisks.html (According to Professor Acquisti, a "person's face is the veritable link between her offline and online identities," and "When we share tagged photos of ourselves online, it becomes possible for others to link our face to our names in situations where we would normally expect anonymity.").

Because photographs, videos, and audio files can convey large amounts of information about children that can make them more vulnerable to behavioral advertising, and possibly put their personal safety at risk as well, these types of information should be included in the definition of personal information.

F. The Definition of Personal Information Should Include Both ZIP+4 and the Combination of Date of Birth, Gender and ZIP Code

The Commission seeks input as to whether the combination of date of birth, gender, and ZIP code provides sufficient information to permit the contacting of a specific individual such that this combination of information should be included in the definition of "personal information." It also asks whether an operator's collection of "ZIP+4" may, in some cases, be the equivalent of a physical address. [114]

Children's Privacy Advocates support the inclusion of both within the definition of personal information. The Commission should include date of birth, ZIP code, and gender because the combination of these seemingly non-personally identifiable pieces of information is often enough to allow advertisers and other operators to identify individuals. One study found that as much as "87% of the US population can be uniquely specified by knowledge of his or her 5-digit ZIP code of residence, gender, and date of birth."[115] Date of birth is often collected on the registration pages for children's websites such as Nick.com and Webkinz.com.

---

[114] 2011 Proposed Rule, *supra* note 36, at 43.

[115] Latanya Sweeney, Abstract, Uniqueness of Simple Demographics in the U.S. Population (Carnegie Mellon Univ. Lab. for Int'l Data Privacy 2000). *See also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L. Rev. 1701, n.4 (2010) (noting that "More recently, Philippe Golle revisited Dr. Sweeney's study, and recalculated the statistics based on year 2000 census data. Dr. Golle could not replicate the earlier 87 percent statistic, but he did calculate that 61 percent of the population in 1990 and 63 percent in 2000 were uniquely identified by ZIP, birth date, and sex.").

The Commission should also add ZIP+4 to the definition of personal information. Similar to geolocation information, one's ZIP+4 information can be as accurate as a street name or even a physical address. More specifically, a ZIP+4 "identifies a geographic segment within the 5-digit [zip code] delivery area, such as a city block, office building, individual high-volume receiver of mail, or any other unit that would aid efficient mail sorting and delivery."[116] In rural areas especially, the ZIP+4 has the potential to identify a single individual. In fact, "some ZIP Codes represent very few addresses (sometimes only one)."[117]

Advertisers and other operators are prepared to use ZIP+4 information to target individuals.[118] Some claim that the greater location accuracy offered by ZIP+4 "permits is offline demographic data (census, etc.) to become part of the online targeting paradigm."[119] Because ZIP+4 can facilitate direct contact with individuals, it should be included in the COPPA Rule's definition of personal information.

III. The Commission Should Adopt Most of the Proposed Revisions to Notice Requirements and Consent Mechanisms

Children's Privacy Advocates support the Commission's efforts to improve notice and consent mechanisms. Parental notice and consent are, as the Commission describes, a core safeguard. For parents who desperately want the tools to protect their children, the new data tracking, profiling and targeting practices pose huge challenges. Parents overwhelmingly believe that they should be able to mediate their children's activities

---

[116] *See* United States Postal Service, Frequently Asked Questions, ZIP Code Information, http://faq.usps.com/eCUstomer/iq/usps/.
[117] U.S. Census Bureau, Geography Division, Zip Coded Tabulation Areas (ZCTAs), http://www.census.gov/geo/ZCTA/zcta.html
[118] Eliot Van Buskirk, *Coming Soon: Web Ads Tailored to Your Zip+4*, Epicenter: Wired.com (June 22, 2010) http://www.wired.com/epicenter/2010/06/coming-soon-web-ads-tailored-to-your-zip-4/all/1.
[119] *Zip+4 Targeting About to Get Real*, Screenwerk http://www.screenwerk.com/2010/06/23/zip-4-targeting-about-to-get-real/.

online. The recent study by danah boyd and others provides powerful evidence that the public demands a robust parental notice and consent framework for the regulation of children's privacy.[120] It found that "on the hot-button issue of child safety, over half of parents preferred an emphasis on better mechanisms for getting parents involved in the issue."[121]

Not only do parents want the tools necessary to effectively mediate their children's use of new technologies, but there is research suggesting that parental mediation strategies can be effective in some circumstances. For example, a 2008 study found that for three different age groups of young Internet users, "the lowest level of

[120] danah boyd, Eszter Hargittai, Jason Schultz, & John Palfrey, *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act*, First Monday (Nov. 7, 2011), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075 ("Overwhelmingly, parents believe that they should have the final say about what their child can do online. When asked who should have final say about whether or not their child should be able to access online services, 93 percent of parents indicated that they themselves should."); *see also* Comments of Mark Andrejevic, University of Iowa, Nov. 27, 2011, http://www.ftc.gov/os/comments/copparulereview2011/00044.html ("I am writing largely in response to comments that I know you are receiving from a research group headed by danah boyd and financed by Microsoft. . . . The authors' see their research as a challenge to public support for age-related restrictions on the tracking of children . . . , but this is refuted by their own findings. It is telling, and perhaps testimony to how this study was funded . . . that the authors frame their key finding in this regard as follows: 'Even when the focus is on data collection, parents are not uniformly in favor of restrictions on what information social network sites can collect about children. While 57 percent would prefer restrictions, even if it means that children in general will be banned from social network sites, 43 percent think that parents should get to choose, even if it means that these sites and services can collect data' (see: http://bit.ly/ParentSurveyCOPPA.). A more accurate way of framing this finding would be to note that a majority of parents favor restrictions on what information social network sites can collect about their children, even if that means children will be banned from such sites. While COPPA may well need to be reformed, it is worth bearing in mind that (unsurprisingly) the general public support age- related restrictions on tracking and advertising.").

[121] boyd, *supra* note 120.

personal information disclosure was consistently found for those participants whose parent actively mediate their online experiences."[122]

While Children's Privacy Advocates generally support the Commission's proposed revisions, we are concerned that given the vast array of complex and rapidly changing techniques being used for data collection, profiling and behavioral advertising, it is sometimes difficult or impossible for parents to fully understand the implications of providing consent. For this reason, the Commission should monitor and evaluate the effectiveness of the rule changes. It should also make clear that where parents are unable to provide consent that is meaningful and informed with respect to a particularly complex practice, the Commission should presume that consent is denied.

A. CDD Supports Making Notice Requirements More Helpful to Parents

For COPPA to be an effective safeguard that empowers parents, operators must provide accurate, understandable, and timely notice. To further this goal, the FTC proposes to put less reliance on online privacy statements ("online notice") and require more effective notice at the time personal information is being collected ("direct notice").[123] Children's Privacy Advocates support this concept. We agree that many of the children's privacy policies are unnecessarily long, confusing and opaque, and as a result, few parents are likely to read them, or understand them if they do.

1. Children's Privacy Advocates Support Clarification that All Operators Must Provide Online Notice

The Study by Sharon Goott Nissim, an independent expert in consumer privacy issues, included as Appendix B, analyzes the privacy policies of the most popular

[122] May O. Lwin, Andrea J.S. Stanaland, & Anthony D. Miyazaki, *Protecting Children's Privacy Online: How Parental Mediation Strategies Affect Website Safeguard Effectiveness,* 84 J. Retailing 205, 213 (2008).
[123] 2011 Proposed Rule, *supra* note 36, at 48.

children's websites. The Nissim study finds that a large number of top children's websites' privacy policies and practices do not fully comply with the current version of the COPPA Rule,[124] confirming the Commission's view that such statements are often under inclusive in ways that may be misleading. She finds for example that:

> [T]he way in which the sites address behaviorally targeted advertising is particularly misleading, as they often disavow engaging in the practice, but then admit that third parties may do so, but assert that those third parties are not covered under the privacy policy. The privacy policies of these third-parties are rarely made available.[125]

Many such entities are currently or will be considered "operators" under the revised COPPA Rule.[126] But as the Nissim study shows, the privacy notices on children's websites provide little or no information about the practices of these operators under the current regulatory regime, Instead, sites' privacy policies commonly include broad disclaimers about the practices of any secondary operators who might be using sites as conduits to collect information about kids. For example, the privacy policy of Ganz, which owns the popular children's website Webkinz World, states:

> [Third-party advertising service providers] may themselves set and access their own tracking technologies and/or they may otherwise have access to information about you. The use of such technology by these third parties is within their control and not ours. Even if Ganz has a relationship with

---

[124] Appendix B at 15.
[125] *Id.* at 5.
[126] 1999 NPRM, *supra* note 5, at 22,752 ("The term 'operator' includes . . . a person who collects or maintains [personal] information through another's website or online service. . . . In determining who is the operator for purposes of the proposed Rule, the Commission will consider such factors as who owns the information, who controls the information, who pays for the collection or maintenance of the information, the pre-existing contractual relationships surrounding the collection or maintenance of the information, and the role of the website or online service in collecting and/or maintaining the information."); Final Rule, Nov. 3, 1999 64 C.F.R. 212 at 59891 ("The Commission believes that an entity's status as an operator or third party under the Rule should be determined not by its characterization as a corporate affiliate, but by its relationship to the information collected under the factors described in the NPR.").

> the third party, it does not control its sites or policies and practices regarding your information.[127]

The policy then tells parents, "If you would like more information about the practices used by third-party advertising service providers and advertisers and to know your choices about not having the information gathered used by these companies, visit http://networkadvertising.org." A visit to that site, however, home of self-regulatory group Network Advertising Initiative, reveals that three of the nine advertising service providers operating on Webkinz World are not even members of this organization.[128] There is thus no notice whatsoever of the practices of these advertising service providers—providers known to engage in behavioral targeting.[129] This result is obviously inconsistent with a law constructed to address "companies . . . attempting to build a wealth of information about you and your family without an adult's approval—a profile that will enable them to target and to entice your children to purchase a range of products."[130]

The Commission's proposed changes to notice requirements should remedy this problem by making clear that the notice requirements "apply to *all* operators of a Web

---

[127] Ganz, Webkinz – General Privacy Policy, http://www.webkinz.com/us_en/privacy_policy.html (last visited Dec. 22, 2011).

[128] A screenshot in the Smith survey of the "Ghostery" tool running over the Webkinz World homepage shows that the following companies or services operate tracking tools on the site: Acerno, Adnetik, Casale Media, Google (DoubleClick, DoubleVerify, DoubleVerify Notice, Google Adsense, and Google Analytics), MediaMath, Microsoft Atlas, Nielsen (NetRatings SiteCensus), Quantcast, and Turn. Appendix A at 11. Of these, Adnetik, Nielsen, and Turn do not appear to be members of the NAI. *See* http://networkadvertising.org/participating/.

[129] Adnetiks' "Audience Investment Management" service "aggregates data from relevant public and private sources, such as proprietary ad server data and third party information from sources like BlueKai, to give advertisers access to defined audience targets over controlled inventory sources." Adnetik, How it Works, http://adnetik.com/how-it-works/ (last visited Dec. 21, 2011). Turn's "Audience Platform" service "enables audiences to be designed and synchronized across multiple media channels and devices, creating a true 1:1 relationship between a marketer's brand and their audience." Turn, Turn Audience Platform: Overview, http://www.turn.com/?page_id=8114 (last visited Dec. 21, 2011).

[130] 144 Cong. Rec. S8483 (statement of Sen. Richard Bryan).

site or online service, rather than permitting the designation of a single operator as the contact point."[131] The FTC's proposal to require all operators to provide contact information—including name, physical address, telephone number, and email address--should ensure that this key information is available to parents.

2. Children's Privacy Advocates Support the Proposal to Simplify Online Privacy Policies with Some Exceptions

While the Nissim study found that many children's privacy policies omitted essential information, it also concluded that many privacy policies "are clearly too complex for the average parent to understand."[132] The Nissim study finds that privacy policies are opaque and confusing in several ways. First, the links to children's privacy policies are often very small and difficult to locate.[133] Second, the privacy policies contain "language that is unclear, difficult to understand, and often internally contradictory."[134] Third, in disclosing how information might be shared with third parties, many privacy policies "do not explain exactly what is shared and with whom, or whether this information could be used to re-identify an individual."[135]

The Commission's proposal would address this problem by requiring that in lieu of the "lengthy—yet potentially under inclusive" privacy policies that are widespread today, the online notice should be simplified to include:

1) what information the operator collects, including whether it enables a child to make personal information publicly available;

2) how the operator uses such information; and

3) the operator's disclosure practices for such information.

---

[131] 2011 Proposed Rule, *supra* note 36, at 49 (emphasis in original).
[132] Appendix B at 4.
[133] *Id.* at 5.
[134] *Id.* at 6.
[135] *Id.* at 12.

Children's Privacy Advocates share the Commission's hope that simplifying online notice requirements will encourage operators to provide more clear, concise descriptions of their information practices. However, we believe that there are two additional types of information that should be disclosed in all children's online privacy policies.

First, we disagree with the Commission's proposal that privacy policies operators should no longer be required to state that operators may not condition a child's participation in an activity on the child's disclosing more PI than is reasonably necessary to participate.[136] This is a very important principle of fair information practices that has been included in COPPA. Ensuring that the online privacy statement includes this information can help to educate parents. It may also prompt them to consider whether in fact the operator complies with the principle. Further, including this information does not unduly expand the length or complexity of privacy policies.

Second, the Commission should require website and online service operators to include information to parents on how their data is secured from potential breaches. As discussed below, data retention policies are important. Again, this notice need not be long and its inclusion could help educate parents.

3. Children's Privacy Advocates Support Proposals for Just-in-Time Direct Notice to Parents

Children's Privacy Advocates generally support the Commission's proposals regarding direct notice to parents.[137] A just-in-time system can help parents understand and make better decisions about whether to allow a specific data collection practice. The proposed revised direct notice requirement will ensure that direct notices to parents are

[136] 2011 Proposed Rule, *supra* note 36, at 49–50.
[137] *Id.* at 52.

clear and uniform, as well as reduce the burden on operators of figuring out what information a direct notice must convey.

B. Children's Privacy Advocates Generally Support the Proposed Revisions to Consent Mechanisms

Children's Privacy Advocates support the Commission's recommendation to eliminate the sliding scale approach commonly referred to as "email plus." Although email plus "was identified as the easiest and least costly for businesses, [it] was also recognized as having the greatest potential for abuse."[138] Moreover, this method of consent was intended to serve as a temporary solution until a better, more reliable mechanism was developed.[139] The time has come to eliminate this "temporary" and ineffective solution. The Commission should not permit widespread circumvention of one of the Rule's core tenets and put children's privacy at risk solely because implementing other mechanisms may come at some cost to businesses. In any event, we have no doubt that this change will encourage innovation and better forms of verifiable parental consent will be developed.

The Commission should also require operators to maintain records of parental consent until a child's account or service has been terminated or lapsed for more than 12 months. Such retention is necessary so that independent auditors, as well as Safe Harbor organizations, can conduct periodic reviews. However, Children's Privacy Advocates do not support the proposal to allow operators to collect a form of government issued identification, such as a driver's license, to verify the identity of parents.[140] Although the proposal would require that this information be deleted immediately after consent is

---

[138] Janine Hiller, France Belanger, Michael Hsiao, & Jung-Min Park, *Pocket Protection*, 45 Am. Bus. L.J. 417, 434 (2008).
[139] Children's Online Privacy Protection Rule, Proposed Rule, 76 Fed. Reg. 19 (Sep. 15, 2011) (to be codified at 16 C.F.R. pt.321) at 66; *see also* FTC's 2010 Roundtable on COPPA, http://www.ftc.gov/bcp/workshops/coppa/index.shtml.
[140] 2011 Proposed Rule, *supra* note 36, at 63–64.

verified (and hence be unverifiable), the serious risks parents' privacy outweigh the benefits of this proposal.

IV. The Commission Should Adopt Limits on Data Retention

The Commission proposes to require that operators establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Specifically, the proposed regulation would limit the retention of "personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected."[141] In addition, when deleting data, operators would have to take reasonable measures to prevent unauthorized access or use.

Children's Privacy Advocates strongly support data retention limits. Without limits, operators can keep children's data indefinitely. And they have the incentive to do so because the more data marketers can associate with an individual's profile, the more valuable that information is to them. Many websites aimed at children, such as Nickelodeon and Disney, do not disclose in their privacy policies how long they retain children's information.[142]

The less data retained, the fewer problems there will be with data breaches. A search of the Privacy Rights Clearinghouse's Chronology of Data Breaches Security Breaches 2005 to the Present[143] found a significant number of breaches over the years that involved information about children. The longer data is detained, the more likely a data breach will have broad-ranging and serious consequences. As Commissioner Brill

---

[141] *Id.* at 78.
[142] *Nick.com Privacy Policy and Online Tracking Data*, Wall Street J. (Sept. 17 2010), http://blogs.wsj.com/wtk-kids/2010/09/17/nickcom/; *Disney.go.com Privacy Policy and Online Tracking Data*, Wall Street J. (Sept. 17 2010), http://blogs.wsj.com/wtk-kids/2010/09/17/disneygocom/.
[143] Privacy Rights Clearinghouse, Chronology of Data Breaches Security Breaches 2005 – Present, http://www.privacyrights.org/data-breach.

recently noted, "If advertisers hold on to data for an unarticulated future use . . . the impact of a data breach is heightened in direct proportion to the amount of data collected."[144]

Even if there is no large-scale data breach, privacy can be threatened "by a slow series of relatively minor acts which gradually begin to add up."[145] As the Commission reported to Congress, "8% of the ID theft complaints in 2010 involved children."[146]

The revised Rule should require that websites or online services that are directed to children or have actual knowledge that the data they are storing came from a child, should delete such personal information within a reasonable timeframe, not to exceed three months. Three months is consistent with Yahoo's original data retention standard announced in 2008.[147] After three months, all personal information as defined by the COPPA Rule should be deleted except for data in aggregate form used only for internal operations.

V. Self-Regulatory Efforts Are Insufficient to Protect Children's Privacy

Children's Privacy Advocates strongly disagree with those who argue that the FTC's proposed revisions are unnecessary because of industry self-regulation. While

---

[144] *FTC Commissioner Brill Warns Advertisers of Potential Harms from Vast Collection of Data; Delivers Message as Featured Speaker at PMA Marketing Law Conference,* Market Watch (Nov 16).

[145] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 769 (2007).

[146] Prepared Statement of the Federal Trade Commission Before the Subcommittee on Social Security of the House Committee on Ways and Means on Child Identity Theft, Plano, Texas (Sept. 1, 2011), http://www.ftc.gov/os/2011/09/110901identitythefttestimony.pdf.

[147] Miguel Helft, *Yahoo Limits Retention of Search Data*, N.Y. Times (Dec. 17, 2008), http://www.nytimes.com/2008/12/18/technology/Internet/18yahoo.html. In April 2011, however, Yahoo increased the data retention period to 18 months. Greg Sterling, *Yahoo Search Data Retention Goes from 90 Days to 18 Months*, Search Engine Land (Apr. 20, 2011), http://searchengineland.com/yahoo-search-data-retention-goes-from-90-days-to-18-months-73899.

industry self-regulation is a valuable complement to government regulation, it needs to be backed up with clear and enforceable rules because most self-regulatory programs are designed to do no more than meet existing legal requirements.

For example, the *Self-Regulatory Principles for Online Behavioral Advertising* developed jointly by the AAAA, ANA, CBBB, DMA and IAB, address the collection and use of children's data under Principle 8, "Sensitive Data." According to this principle,

> Entities should 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 directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.[148]

Similarly, the Safe Harbor programs that are approved by the FTC pursuant to COPPA Rule 312.10 need only meet "substantially similar requirements that provide the same or greater protections for children" as contained in the COPPA Rule. Thus, it is not realistic to expect that a self-regulatory scheme will require more than is required by law.

There are many other well-known problems with the use of voluntary self-regulation. Not all companies participate in self-regulatory schemes. Moreover, many that say they do in fact do not comply. The BBB recently found six companies in violation of the principles.[149] Although in this case the companies agreed to bring their practices into compliance, there is no meaningful enforcement mechanism for companies

---

[148] http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

[149] Hayley Tsukayama, *Advertisers Release First Self-Regulation Results,* Washington Post: Post Tech (Nov. 8, 2011), http://www.washingtonpost.com/blogs/post-tech/post/advertisers-release-first-self-regulation-results/2011/11/08/gIQA26Cf2M_blog.html; *Accountability Program Achieves Voluntary Compliance with Online Behavioral Advertising Self-Regulation*, Better Business Bureau (Nov. 8, 2011), http://www.bbb.org/us/article/accountability-program-achieves-voluntary-compliance-with-online-behavioral-advertising-self-regulation-30529.

that choose not to comply. Moreover, a recent study by researchers at Carnegie Mellon University found that "two years after the DAA published its Self-Regulatory Principles, there are still numerous instances of non-compliance."[150] Specifically, the study found widespread non-compliance with notice and opt-out requirements.[151] Other research conducted at the Stanford Center for Internet and Society revealed that only 9.9% of third-party ads on the top 500 U.S. websites included an "AdChoices" link in or around the ad, required under the DAA's enhanced notice guidelines.[152] Given the inadequacies of the existing self-regulatory programs, they simply cannot be relied upon to protect children's privacy.

Conclusion

Since the initial COPPA Rule was adopted in 1999, the techniques used to track, profile, identify, target, and retarget individuals in the digital environment have become highly sophisticated. Through web analytics, conversation targeting, and other forms of surveillance, marketers can now track individuals online, across media, and in the real world, monitoring their interactions, social relationships, and locations. The dramatic growth of the digital marketplace and its increasing role in the lives of children make it imperative that the COPPA Rule be revised to ensure that the Rule provides effective safeguards for protecting children's privacy.

Children's Privacy Advocates generally support the Commission's proposed revisions and urge it to act quickly in revising the Rule along the lines proposed. In particular, we support the Commission's proposal to expand and clarify the definition of

---

[150] Saranga Komanduri, Richard Shay, Greg Norcie, Blase Ur, & Lorrie Faith Cranor, *Ad Choices? Compliance with Online Behavioral Advertising Notice and Choice Requirements*, Cy Lab Carnegie Mellon University (Oct. 7 2011) http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf.

[151] *See Id.*

[152] Jonathan Mayer, *Tracking the Trackers: The AdChoices Icon*, Stanford Center for Internet and Society (Aug. 17, 2011), http://cyberlaw.stanford.edu/node/6714.

"personal information." The proposed inclusion of persistent identifiers is particularly important to limit the extensive tracking and behavioral targeting of children already occurring without the knowledge and consent of parents, while still ensuring that operator have data needed to support internal operations. Children's Privacy Advocates urge the Commission to improve the notice and consent procedures as proposed in these comments.

Of counsel:

Ariel Gursky
Law Student
Georgetown Law

Dated: December 23, 2011

Respectfully submitted,

/s/ Angela J. Campbell

Angela J. Campbell,
Laura M. Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535

Counsel for Center for Digital Democracy

A Survey of Web Tracking Technologies Used by Popular Children's Web Sites

Survey conducted by Richard M. Smith, Boston Software Forensics[1]

Introduction

I was asked to do a survey of 54 leading Web sites that are primarily intended for use by children, in order to understand what Web tracking technologies are employed by the sites. These Web tracking technologies are used across the Web to provide targeted advertising to visitors of Web sites. The technologies that were investigated as part of the survey include:

- Web browser cookies
- IP addresses
- Web bugs
- Behavioral targeting
- Internet advertisements
- Flash cookies
- Web analytics

Survey Results

To conduct this survey, the Fiddler tool (http://fiddler2.com/fiddler2/) was used to capture all Web requests and responses when a browser visits each of the children's Web sites of the survey. A driver script was created to automatically visit the home page of each Web site so that Fiddler was able to capture Web requests and responses. To eliminate interactions between Web sites, the browser cache, cookies, and Flash cookies were cleared out before visiting a new home page.

An analysis script was then created to understand which tracking technologies are being used at the children's Web sites. This analysis script worked from log files created by the Fiddler tool that contain all Web requests and responses between a browser and a Web site.

In addition, for the Web sites that allow for registration, test accounts were set up in order to observe how registration data might be used in return visits to a Web site.

[1] Prepared for inclusion as an appendix accompanying comments of Center for Digital Democracy, et al. on the Federal Trade Commission's proposal to amend the Children's Privacy Protection Rule to Respond to Changes in Online Technology. 76 Fed. Reg. 59804 (Sept. 29, 2011) (to be codified at 16 C.F.R. pt. 312).

The following table summarizes the results of the survey:

Tracking technology	**Web site count**	**Percentage**
First-party cookies	44	81%
Internet ad network tracking	38	70%
Behavioral ad targeting	26	48%
Web analytics	45	83%
Registration data	23	42%

As this table makes clear, Web tracking technologies are used extensively at children's Web sites. It appears that children's Web sites have embraced standard Web tracking technologies as much as the rest of the Web.

Behavioral targeting (BT) for Internet ads has generated the most controversy in the past. Behavioral targeting tracks a person over time as they surf the Internet, to understand what kinds of products and services they seem to be interested in based on the Web pages that they visit. Internet ads are then displayed on Web sites based on personal profiles created by Behavioral targeting services.

In many cases, Behavioral targeting tracking is done by specialized Internet marketing vendors. Their profiling data are then used for selecting ads, while ad delivery is done by traditional Internet ad networks. In other cases, Internet ad networks will do behavioral targeting tracking, ad selection, and ad delivery.

This table lists children's Web sites that appear to be using behavioral targeting technologies:[2]

BT company	Children's Web site	Brief product description
[X+1]	www.chuckecheese.com	"[x+1] pioneered the DMP [data management platform] to empower all manner of data, including demographics, purchase intent, and buyer propensity. This gives marketers and agencies a powerful tool for customer-centric marketing – allowing them to reach just those online visitors who are at the intersection of interest, need and purchase readiness." http://www.xplusone.com/solutions_dmp.php

[2] To determine if a Web site is using behavioral ad targeting, the analysis script looked for JavaScript files and Web bugs from companies who offer behavioral ad targeting services.

Adnetik	www.coolmath-games.com	"AIM aggregates data from relevant public and private sources, such as proprietary ad server data and third party information from sources like BlueKai, to give advertisers access to defined audience targets over controlled inventory sources." http://adnetik.com/how-it-works/
Adobe	www.neopets.com www.nick.com www.nickjr.com	"Demdex's turn-key audience management solutions make implementing a dynamic, multi-channel data strategy cost-effective and easy. We empower your company to create a "Data Bank" of audiences with data captured from your web properties, purchased from third-party data sellers or exchanges, and generated from your ad campaigns." http://www.demdex.com/
AudienceScience	disney.go.com funschool.kaboose.com	"AudienceScience is the largest and most trusted audience aggregator in the world. As an early innovator of online advertising technology, AudienceScience continues to revolutionize the industry, enabling universal access to audiences and driving digital marketing success with The Audience Delivery Solution. Since 1999, AudienceScience has been developing technology to provide advertisers, agencies and publishers the ability to define, reach and learn about their key audiences." http://www.audiencescience.com/technology
BlueKai	www.coolmath-games.com www.ganzworld.com www.roblox.com www.sesamestreet.org	"BlueKai's data-centric approach to audience targeting has made the marketer's dream of 'reaching an audience anytime anywhere' a reality." http://www.bluekai.com/
Brilig	www.pencilkids.com	"Brilig is the first cooperative data marketplace for online display advertising. Unlike other legacy data marketplaces or exchanges, Brilig data is sourced cooperatively and normalized from hundreds or even thousands of discrete databases — many of which have never been 'connected' to digital display advertising. This crowd-sourced, 'desiloification' of the world's data is completely unique to Brilig." http://www.brilig.com/platform.php

Casale Media	www.bakugan.com www.coolmath-games.com www.ganzworld.com	"Successful campaigns begin with the right audience. And knowing who that audience is begins with solid research. Our targeting platform seamlessly integrates survey, panel and actual product consumption data from leading market research providers including Nielsen, MRI, Polk, Equifax and comScore to make identifying (and then reaching) your best customers across our wide-reaching network a snap." http://www.casalemedia.com/audience/
CrowdScience	www.cartoonnetwork.com	"Most sites just scratch the surface when trying to understand their audiences. They spend a lot of time comparing their high level audience to other sites, but lack methods for understanding the varied audiences inside their own site sections or sub-sites. If you dig deeper, you'll find a whole new world of unique demographic and behavioral traits about your audience, providing new opportunities to grow, target and monetize your business. AUDIENCE by Crowd Science provides publishers with scientifically rigorous technology and best-in-class survey research…." http://crowdscience.com/products/audience_demographics
Datalogix	www.ganzworld.com www.nick.com	"DLX operates the only ad network 100% focused on targeting based on purchase data and measuring digital campaigns based on ROI, not clicks. Convert your CRM database into an online audience, and reach your existing customers anywhere they are online with the right message. Take your best customers and use our $1 trillion dollars in consumer spending to identify 'Spend-A-Like' prospects across our network. DLX Net programs measure campaign results back to offline AND online sales. We deliver a hard ROI on every campaign." http://datalogix.com/digital-media/
FetchBack	marvelkids.marvel.com www.animaljam.com	"What is Retargeting? "In the simplest terms, retargeting means putting messages in front of lost prospects who've left your Web site in order to attract them back and convert – finish the purchase, sign up for the

		newsletter, or whatever action you're looking for." http://www.fetchback.com/retargeting.html
Interclick	www.littletikes.com	"Interclick's years of experience in behavioral targeting gave us a key insight: first and second generation data targeting platforms were falling behind the evolution of the online advertising market. In their time, these platforms were important industry innovations. But largely based on older technologies, they had trouble with new developments in data, inventory and messaging." http://www.interclick.com/our-technology/why-osm.aspx
Lotame	kids.nationalgeographic.com	"Crowd Control's sophisticated algorithms and expansive database of audience data enables publishers and advertisers to directly monetize data and find the right audience for online marketing campaigns." http://www.lotame.com/platform/
Quantcast	kids.nationalgeographic.com www.4kids.tv www.coolmath-games.com www.fantage.com www.funbrain.com www.kidswb.com www.miniclip.com www.nick.com www.nickjr.com www.poptropica.com www.secretbuilders.com www.sesamestreet.org www.sproutonline.com www.miniclip.com www.secretbuilders.com	"Use Quantcast audience segments to group your audiences any way you like. Define the custom audiences advertisers want, and deliver more of your hard-won audience base. "Quantcast Demographics "Segment out specific audiences you want to sell across your content. Adjust the composition of your audiences to index higher and target audiences that were previously challenging to deliver." http://www.quantcast.com/audience/reach-audience-for-media-sellers
Rapleaf	www.ganzworld.com	"Personalized Emails "Customize emails to each member of your audience. Use gender, location, and interests to write emails that are meaningful and relevant. "Recommendation Systems "Recommend music, movies, articles, and associates that are interesting to your users. Save their time, and make the best first impression."

		https://www.rapleaf.com/how_it_works
Red Aril	www.pencilkids.com	"Our solution features the Red Aril Data Management and Audience Optimization Platform (DMP) supported by our experienced, professional services team. The Red Aril Platform was designed from the outset to manage today's intense marketing and advertising environment - high data volumes within a real-time environment. To ensure full leverage of our innovative platform, we offer our client's a flexible service model (self – hybrid – full)." http://www.redaril.com/solution
Tacoda	kids.aol.com	"Age, gender, income, kids – it's the meat and potatoes of targeting. "User/Household: Target users based on attributes from user registration or third-party data (e.g. age, gender, income, kids). "Site: Place your ads on the sites that are visited most frequently by your desired audience. We aggregate our inventory by demographic and psychographic attributes – based on comScore data. You can, for example, place your ad on sites that are visited by users who attended college, users who applied offline for a credit card in the last six months, user who traveled domestically over six times in the last six months, and many more." http://advertising.aol.com/platforms/targeting
TARGUSinfo	www.ganzworld.com www.nick.com www.roblox.com	"Verified Audience Targeting Data "AdAdvisor®, powered by TARGUSinfo, is an audience targeting solution allowing marketers to deliver the most relevant display advertisements to online consumers. With TARGUSinfo's proprietary linking logic and the power of ElementOne® Analytics, AdAdvisor helps advertisers instantly connect consumers to attributes and propensities such as demographics, lifestyle preferences and brand affinities." http://www.targusinfo.com/solutions/scoring/optimization/

Turn	www.littletikes.com	"Turn Audience Platform: Overview For Global 2,000 brands and leading advertising agencies, the Turn Audience Platform is the first data management platform (DMP) that centralizes audience data from any source – online or offline, first-party or third-party – in a scalable, actionable repository." http://www.turn.com/?page_id=8114

Cookies

The foundation for Web tracking is the Web browser cookie. A cookie is a small amount of text that a Web site sends to a Web browser when a Web browser requests a Web page or other type of Web content, such as image or script files. A cookie is generated by a Web site by including a set-cookie header line as part of the response headers. The cookie text is then stored on the user's hard drive. In the future, when the browser returns to the Web site, the cookie text is sent back to the Web site as a header line in the request for a Web page or other Web content.

A Web site is allowed to store more than one cookie on a user's hard drive. It is not uncommon to see Web sites use 5 to 10 cookies. The actual meaning of the content of a cookie is determined by the Web site that sets them. Browsers do not try to interpret cookie values.

Cookies are also private to the Web sites that set them. That is, one Web site cannot read the cookies set by other Web sites. A Web site is only allowed to set and read its own cookies.

Here is an example of a cookie being set up the Disney Web site disney.go.com:

Set-Cookie: SWID=6665D324-0FC7-4B7D-ACBB-8EF50D47E21E; path=/; expires=Sun, 30-Oct-2031 22:40:15 GMT; domain=.go.com;

The name of the cookie is "SWID" and its value is "6665D324-0FC7-4B7D-ACBB-8EF50D47E21E." The cookie is set to expire in the year 2031. Because it is unlikely that the user's computer will still be operation in the year 2031, the cookie is effectively set to live for the life of the computer. The domain parameter specifies that the cookie value is to be returned to any Disney Web server that has a name ending with the string ".go.com."

From its appearance, the Disney SWID cookie is likely a unique ID number that identifies a particular Web browser. ID numbers are typically used in cookies to track the activities of a person using a particular Web browser over time.

A useful analogy for this type of tracking cookie is a membership card. The first time someone visits a Web site, they are given a membership card for the Web site in the form of a cookie. The membership number on the card is the unique ID number of the cookie. The membership card and number are stored away on the user's hard drive. Each time a person returns to the Web site, their membership card number is sent back to the Web site, allowing the Web site to track what a person has been doing at the Web site over time.

The history of the Web pages that a person has visited over time is sometimes referred to as a click-stream. This name came about because people typically go from one page to another on a Web site by clicking on links. Hence the series of link clicks is called a click-stream.

The following information typically gets recorded for a click-stream in a database table at the Web site:

1. The date and time that a Web page is requested
2. The IP address of the browser requesting the Web page
3. The cookie ID number assigned to the browser
4. The URL (Web address) of the Web page being requested
5. The type of the browser requesting the Web page

Third-Party Cookies and Web Bugs

Because of the underlying architecture of the Web, the components of a Web page can come from many different Web servers run by multiple vendors. For example, at the nick.com home page, more than 250 requests for components are made to about 25 different Web servers. Many of these Web servers are not run by nick.com itself, but by third-party vendors such as Internet ad networks, content delivery networks for multimedia files, and Web analytic companies. Web components fetched from these many servers include HTML content, script files, style sheets, images, and video files.

Just like a Web site itself, a third-party vendor can use cookies when a browser makes a request for a Web page component to its servers. These cookies are known as third-party cookies since they go back and forth to a Web server run by a third-party vendor. A first-party cookie is a cookie of the Web site being actually visited.

For example, nick.com uses the DoubleClick ad network to show banner ads at the nick.com Web site. An example set of cookies set by a DoubleClick server looks something like this:

```
id=2276c2a9690100a4  t=132319949  et=531  cs=jggc1g16
```

Presumably the cookie named "id" contains a unique tracking id number for the DoubleClick ad network.

Using the membership analogy from the previous section, when a child visits the nick.com Web site, they quietly become members of both the nick.com Web site and the DoubleClick ad network.

When visiting the nick.com Web site with all cookies cleared out from a browser, at least 6 cookies are set by different vendors, all which appear to contain unique tracking id numbers in them.

When a Web page component is being fetched from a third-party server, a browser will also send the URL of the Web page that the component is part of to the server as part of the request for the component. This URL is sent as a header line in the request and is known as the referring URL or referrer.

Using the referring URL, an Internet ad network can then keep track of the Web pages that someone visits and use this information for ad targeting purposes. However, unlike a single Web site that only gets to track click-stream data on their own Web site, an Internet ad network can do tracking of individuals across many different Web sites that are part of the ad network. This multi-site tracking ability provides more even more data to develop profiles of individuals for ad targeting purposes.

Another tracking technology related to third-party cookies is called a Web bug. Web bugs are also known as Web beacons, clear pixels, tracking pixels, etc. They are invisible images of a Web page that are used exclusively for tracking purposes. Web bugs are typically generated by script files included on a Web page by the Web site owner. The script files generate hidden images and provide tracking information in the URLs of the Web bug images. Web bugs make for enhanced tracking by a third-party vendor because the Web site owner can provide information about a Web site visitor to the third-party vendor based on what it knows from the Web site cookie.

For example, at the nick.com home page, Web bugs are created for the following third-party vendors:

- Google Analytics
- Adobe Analytics
- DoubleClick
- comScore
- The Nielsen Company

Web bugs have a number of different uses on a Web site. One use is to collect data for creating aggregate statistics about the use of the Web site. These statistics can include:

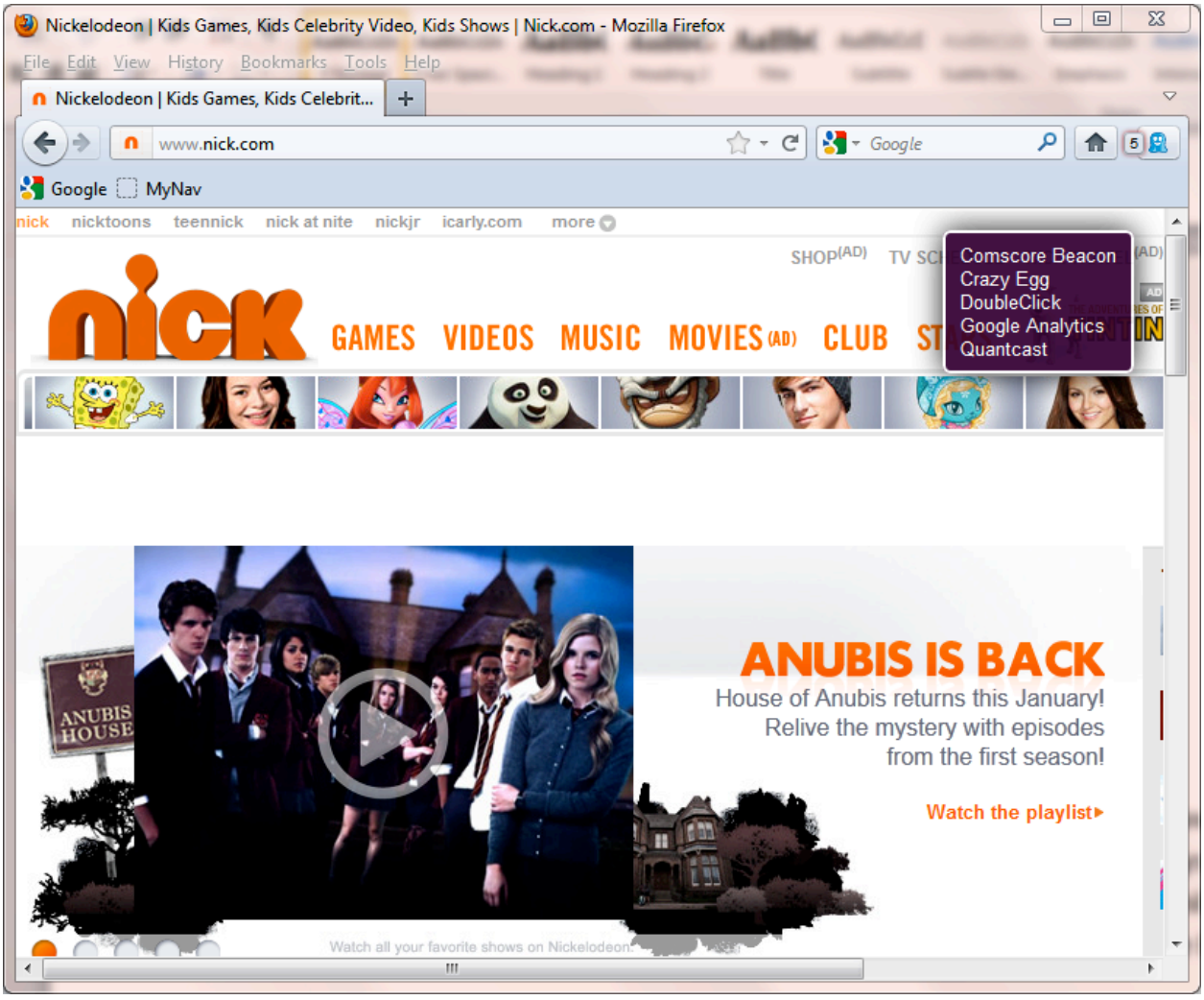
- The most popular Web pages of a Web site
- The number of visitors based on the time of the day
- What Web sites visitors are coming from to get to the Web site
- Etc.

This collection of aggregate statistics is known in the industry as Web analytics. Two companies that provide popular Web analytic services to Web sites are Adobe and Google.

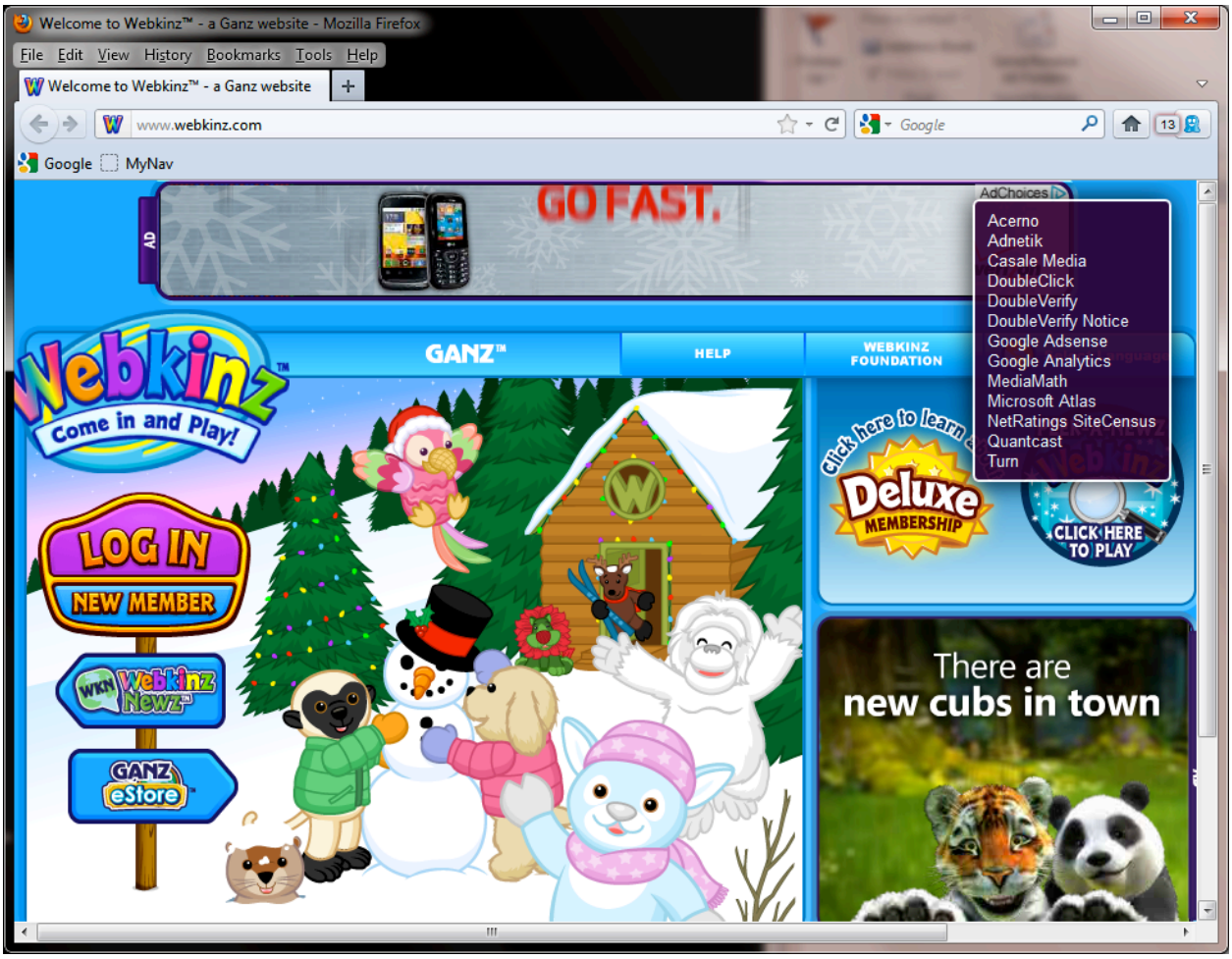
Internet ad networks also use Web bugs to collect data for both gathering aggregate statistics about visitors seeing their ads as well as collecting additional data for ad tracking purposes. This second use of Web bugs targets individual visitors to a Web site as opposed to looking at group behavior as is done with Web analytics.

Although third-party tracking technologies are typically invisible to person visiting a Web site, there are a number of browser tools that show when these technologies are being employed at a Web site. One such tool is Ghostery. The tool can be downloaded at no charge from http://www.ghostery.com/.

For example, Ghostery finds 5 Web bugs at the nick.com home page. These Web bugs provide data back to Comscore, Crazy Egg, DoubleClick, Google, and Quantcast:



Ghostery shows even more tracking being done at the Webkinz.com home page:



Flash Cookies

The Web standard for displaying video and animations on Web sites is Adobe Flash. Adobe Flash is a plug-in for most popular Web browsers that allows small applications to be run inside of Web pages. Popular uses for Flash on Web sites for children are to show short videos and play games.

Like Web pages, Flash applications can store data on a user's local hard drive using a Flash technology called "local storage objects." These Flash local storage objects have been nicknamed as Flash cookies since they can be used for tracking purposes in a similar manner as browser cookies.

Flash cookies have developed somewhat of a tarnished reputation because they are even more hidden than browser cookies. While browser cookies are relatively easy to remove from the local hard drive using the options or settings dialog of a browser, clearing out Flash cookies is more involved.

A number of Internet advertising networks, utilizing the hidden nature of Flash cookies, have turned to Flash cookies to recreate browser cookies that were deleted by a user to try to stop Web tracking. (See FTC Settles with Online Advertiser over Flash Cookie Use - http://blogs.wsj.com/digits/2011/11/08/ftc-settles-with-online-advertiser-over-flash-cookie-use/).

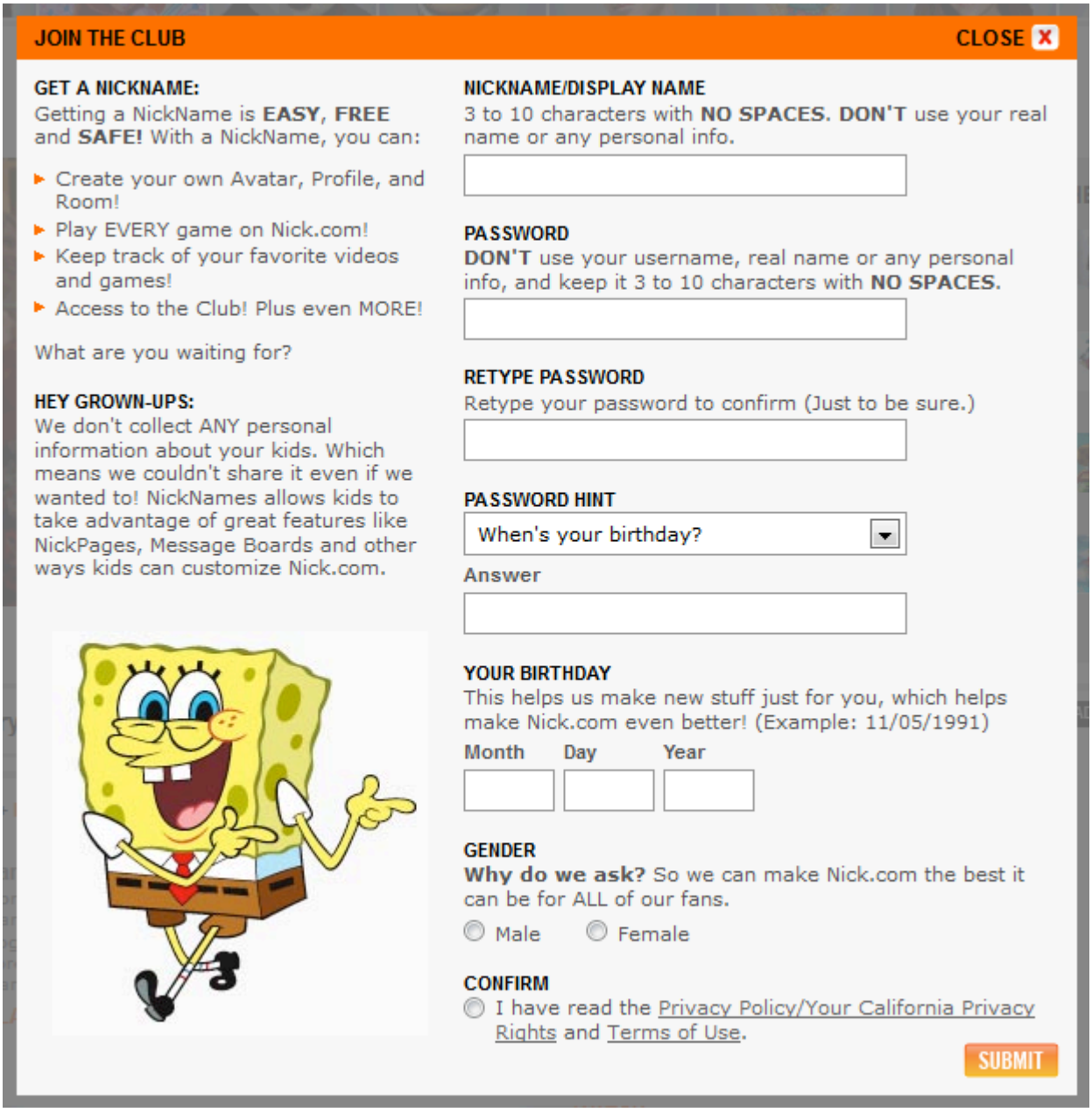
Just like a browser cookie, a Flash cookie can contain a unique ID number for tracking purposes. A number of Web sites for children disclose this kind of tracking in their privacy policies:

> http://www.miniclip.com/games/en/privacy-policy.php
>
> "Third parties and or Miniclip may be placing and reading standard and or flash cookies on your browser and machine."
>
> http://www.ganzworld.com/privacy-policy/
>
> "We may collect such information through unique identifiers such as cookies (which may be HTML files, Flash files, or other technology)."
>
> http://corporate.disney.go.com/corporate/pp.html
>
> "We collect information through technology, such as cookies, Flash cookies and Web beacons."

Registration Data

Another method of getting ad targeting data is simply to ask a child for it. Many Web sites for children allow a child to set up an account at a Web site. As part of the sign-up process, a child may be asked to provide demographic information such as gender and age.

For example, here is the sign-up form for nick.com:



This form asks for both a birthdate and gender. Once this information is submitted to nick.com, it will be associated with the nick.com cookie in a database at nick.com. Later on the information can be used for ad targeting purposes at the nick.com Web site and potential other Web sites.

IP Addresses

Another source of tracking data at Web sites is IP addresses. IP addresses are a necessary part of the technology that two computers require in order to communicate under the Internet. An IP address identifies a computer on the Internet in much the same way that a phone number identifies a phone on the phone network.

For example, when a Web browser is told to download the home page disney.go.com, it will send a request to the IP address 68.71.208.76, which is the IP address assigned to the disney.go.com server. To get this IP address, a browser will do what is known as a "DNS lookup" on the disney.go.com server name. The DNS system is a global system for turning host names that people use into IP addresses that computers use. The DNS system acts like a 411 system for the Internet.

Once a browser has the IP address of a disney.go.com server, it will send a short message in the form of an "HTTP GET" request for the home page of disney.go.com. Included in this request is the following information:

- The URL of the disney.go.com home page.
- The IP address of the user's computer
- The go.com cookies, if any
- A string indicating the type and version number of the Web browser
- The referring URL if any

The IP address of the user's computer is necessary in order for the disney.go.com Web server to know where to send the contents of the home page back to. Taking the IP-address-as-a-phone-number analogy a bit further, caller ID must always be turned on, in order for a Web server to respond to a browser.

Technically, in most America homes, the IP address that a Web server receives is the IP address of the Cable or DSL modem in the home. This is the public facing IP address of the home. All computers of a home that go through this cable or DSL modem will share the same public IP address. Each computer using the modem is giving local IP addresses that are only known by the computer itself and the modem or wireless router of the home.

The IP address of the cable or DSL modem is assigned by an Internet Service Provider (ISP) when the modem is first turned on. The IP address comes from a pool of available IP addresses owned by the ISP. Depending on the policies of the ISP, the same IP address might always be assigned to a subscriber, or it may periodically change. Regardless, an ISP will keep records of which IP addresses are assigned to which customers. These records are kept up to date as IP addresses assignments change at customer modems.

IP addresses are used for a number of key tracking purposes by Web sites. One use is to get the approximate geographic location of a computer based on its IP address. Since blocks of IP addresses tend to get used in particular areas, databases of IP address locations are relatively easy to build. A number of free services are available for doing location tracking. Here is one example:

http://ipinfodb.com/my_ip_location.php

Internet ad networks make use of geographic location information to target ads for advertisers who only want to have their ads shown in particular areas of the country. For example, a fast-food chain might choose to show ads only to children who live in Zip codes that have restaurants of the chain.

Putting it All Together: Ad-Targeting Profiles

A primary reason for all this data collection on Web sites is to sell more advertising at higher prices. Children Web sites pitch the idea to advertisers that ads can be targeted to individual children who come to the Web sites, based on demographic variables such as gender, age, and geographic location. Web sites can charge a higher price for these demographically targeted ads under the theory that children who are unlikely to purchase a product will not be shown ads for these products.

In the industry, the use of Web tracking data is known as behavioral targeting or interest-based targeting.

Here are some examples of the targeting pitch made to advertisers by children's Web sites and advertising technology companies:

> http://www.mattel.com/advertise
>
> Advertise with Mattel
>
> "Highly-targeted boy and girl market segments with above-average click-through rates"
>
> http://corporate.disney.go.com/corporate/pp_online-tracking-advertising.html
>
> Online Tracking and Advertising
>
> "Advertisers and third parties also may collect information about your activity on our sites and applications and on third-party sites and applications using tracking technologies. Tracking data collected by these advertisers and third parties is used to decide which ads you see both on our sites and applications and on third-party sites and applications."
>
> http://www.quantcast.com/

Behavioral targeting is based on building a profile for each visitor to a Web site. The data of a profile are typically stored in a database belonging to a Web site, Internet advertising network, or a vendor who specializes in behavioral tracking. A profile is created for a visitor the first time they come a Web site. The profile is identified by an id number stored in a browser cookie.

An Internet ad network may do its own behavioral profiling to target ads. However, there are many companies in the Internet marketing industry that specialize in behavioral targeting. These companies build behavioral profiles, and their targeting data drive ad selection at more traditional Internet ad networks.

The following sources of data are used to construct a visitor profile over time:

- The URLs of the click-stream for the visitor, which indicate the type of content that the visitor is interested in
- The IP address of the visitor
- Registration data supplied by the visitor
- Searches done by a visitor at a Web site
- Data from other Web sites that are collected by an ad network or a behavioral tracking company

From this data, a Web site can use data mining techniques to draw inferences about a particular person using the Web site. For example, at nick.com, if a child plays the Power Ranger game at the same Web site URL on a regular basis, they might conclude that this child is a boy. On the other hand, if the child instead goes to the "Dress Me Up" Web page, then they are likely a girl.

Also, based on the Web pages being visited by a child, a Web site may also be able to determine the approximate age of the child.

These two pieces of demographic information, gender and age, can then be used by a Web site to select the ads being shown to a child as they go around a Web site. Children are divided into different segments based on their gender and age and ads are targeted based on these segments.

A child's profile in a server-side database holds this demographic information, plus their approximate geographic location, and ratings of likely categories of products that they might be interesting buying. Categories might include things like video games, dolls, movies, etc.

In addition, to using the profile data on their own sites to target ads, Web sites may also "rent out" their profile data to other web sites for ad targeting purposes. For example, here is how AudienceScience describes their data revenue sharing service to prospective Web sites:

> http://www.audiencescience.com/technology/publishers/audience-syndication
>
> Here's how Audience Syndication with AudienceScience works. Our targeting technology tracks anonymous audience behaviors and stores this information in massive databases. In fact, AudienceScience currently tracks and manages trillions of behaviors a day from 386 million unique Internet users.
>
> We make this audience data available to Web advertisers and publishers through our AudienceScience® Network. Within the network, you can import audience behaviors, swapping and sharing with other leading publishers. The result: Your audience data becomes a powerful source of income.

Children Web sites that use the AudienceScience service include Disney properties such as funschool.kaboose.com and disney.go.com.

AudienceScience also provides an informational Web site that describes all the different ways that their behavioral targeting service is able to profile people and place them into segments for ad targeting:

> http://www.audiencetargeting.com/

The demographic categories, which attempt to segment people by gender, age (including children under the age of 18), and household income, are particularly interesting:

> http://www.audiencetargeting.com/demographics.jsp#HHI

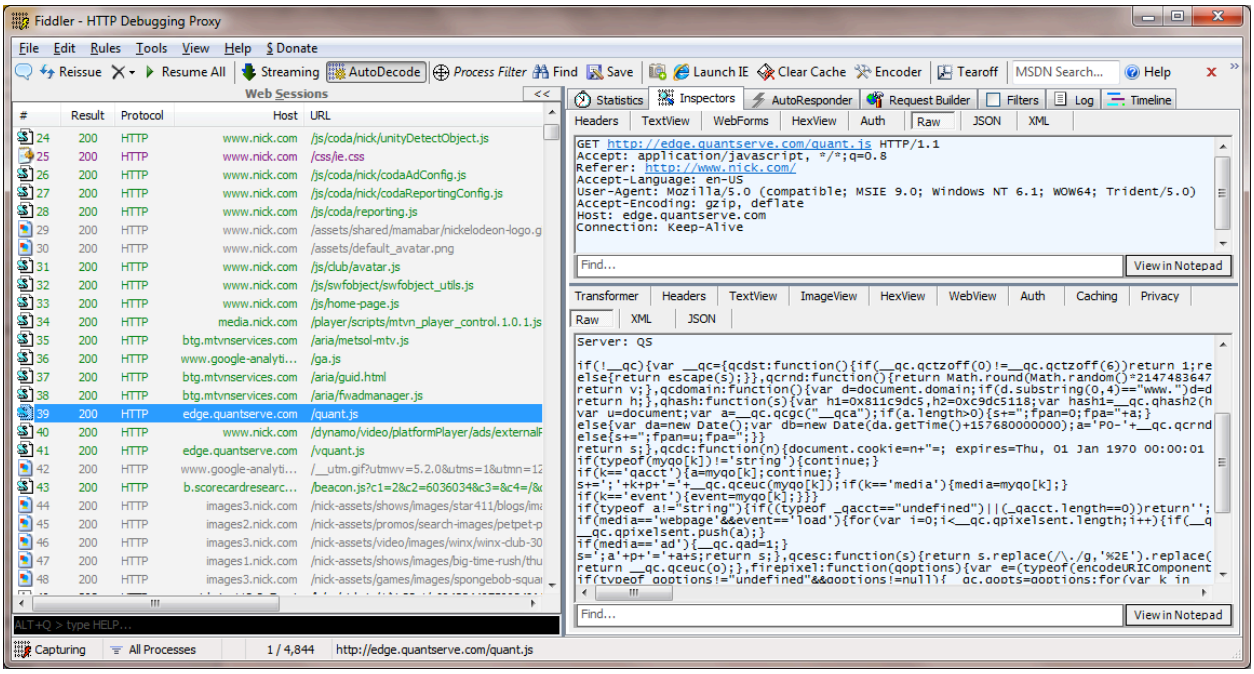
Another demographic category is Hispanic Internet shoppers:

> http://www.audiencetargeting.com/hispanic.jsp#Lifestyle

Observing the ad tracking process

The process of constructing ad-targeting profiles does not always happen in the server-side databases of Web sites and ad technology companies. In some cases, tracking data are exchanged through a child's own Web browser. Using a diagnostic tool such as Fiddler, it is possible to observe the actual process when tracking data are transferred from one server to another through a browser.

This screen shot from Fiddler shows a small portion of the more than 250 transactions between 25 Web servers and a Web browser when visiting the nick.com home page:



The left panel of the Fiddler window shows about 25 of the Web requests made by a browser at the nick.com home page. The transactions are numbered from 24 to 48. In particular, the left panel shows a browser fetching analytic and advertising script files from nick.com, Google, comScore, and QuantCast.

In one example of a data transfer, when a child logs into their account at the nick.com Web site, their registration data is sent back to their browser in a JavaScript file. Here is an example of edited demographic data:

http://www.nick.com/common/login/check.jhtml

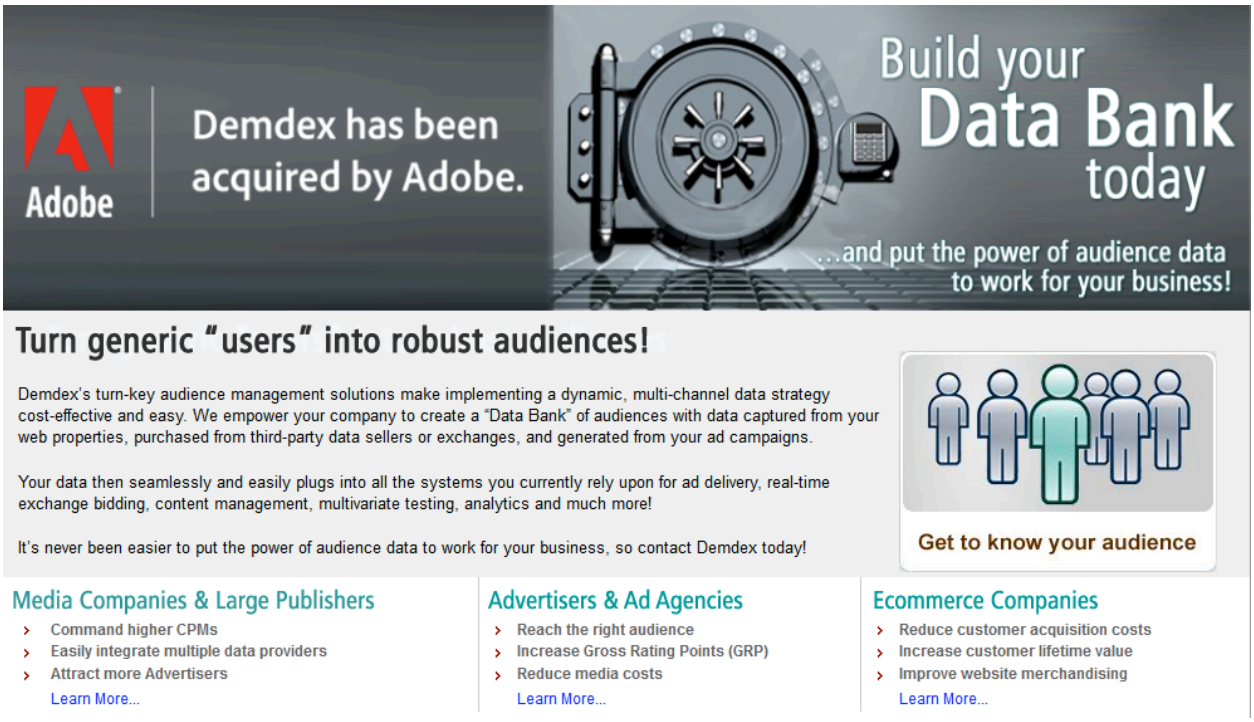
```
var result = {
loggedIn:'true',
loginResult:'1',
loginStatus:'1',
nickName:'FI…',
loginType:'',
```

```
screenName:'FI…',
nickPoints:'500',
eventMode:'false',
messages:'0',
userID:'…',
gender:'Male',
created:'2011-11-09',
age:'12 years 1 month',
approved:'A',
avatar:'m_0001_0001_0001_0001_0001',
gamesResult:'OK',
gamesMsg:'',
userAge:'',
nickBirthday:'',
nickAge:''
};
NICK.request.lstnrs["wwwnickcomcommonlogincheckjhtml1"](result);
```

JavaScript code then places some of the demographic information into a Web bug and transmits the data to Demdex, an advertising tracking company recently purchased by Adobe. Here is an example of a Web bug URL with gender information ("gen=m") that is sent to Demdex:

http://dpm.demdex.net/demdot.jpg?et:dpm|dpid:21|data:seg=037&gen=m

Here is how Demdex describes their tracking services:



In another example at the Ganzworld.com Web site, location information is used for ad-targeting purposes. A script file for a banner ad from the Tribal Fusion ad network includes location information down to the Zip code level. Here is how this location information is generated in the script file:

```
var tf_state       = 'Massachusetts';
var tf_city       = 'Boston';
var tf_zipcode       = '02116';
```

This location information was generated for a Comcast IP address and is accurate within about 1 mile.

In a second Tribal Fusion script file, it is possible to see how Web site visitors are "segmented" based on their age and gender:

http://cdn5.tribalfusion.com/media/2516896//frm.html

```
var segMap = [
            [ 4038049689,  "c9_ta=18-20" ],
            [ 4038049687,  "c9_ta=21-24" ],
            [ 4038049711,  "c9_ta=25-34" ],
            [ 4038049704,  "c9_ta=35-44" ],
            [ 4038049724,  "c9_ta=45-54" ],
            [ 4038049718,  "c9_ta=55-64" ],
            [ 4038049712,  "c9_ta=65+"   ],
            [ 4038049742,  "c9_tg=m"     ],
            [ 4038049733,   "c9_tg=f"    ]
        ];

function searchIndex(segMap, seg)
{
 var val;
 for (var i = 0; i < segMap.length; i++)
  {
   if (segMap[i][0] == seg)
    {
     val = segMap[i][1];
     break;
    }
  }
 return val;
}
```

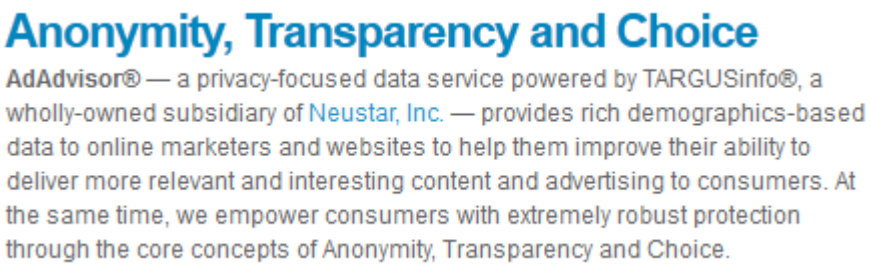
Another example of demographic information being exchanged in a Web browser is the AdAdvisor service from Neustar. A Web site that is a customer of the Neustar service simply fetches a JavaScript data file using script code that runs in a browser. The data file comes back with basic demographic information about a site visitor based on their adadvisor.net cookie and data collected at other Web sites. Here is what this data file might look like:

http://adadvisor.net/adscores/g.json?sid=9233633946

```
Targus.parseInfo({"targus": { "segment": "037", "zip": "{%zip}", "age":
"1987", "gender": "M" } });
```

Here is how Neustart describes the AdAdvisor service:

http://www.adadvisor.net/



Web Tracking and Web Site Privacy Policies

Many of the children's Web sites in this survey include information in the online privacy policies that describe the Web tracking technologies used on their sites. In general, the descriptions are somewhat simplistic explanations of very complex technologies. In addition, the privacy policies do not describe the scope of the tracking that is being done at children's Web sites. For example, Ghostery shows five different trackers on the home page of the Disney Web site http://funschool.kaboose.com/.

Here are three examples of these explanations of Web tracking technologies:

http://www.nick.com/info/privacy-policy.html

Cookies and Log Data

Unique identifiers such as cookies (which may be html files, Flash files, or other technology), web beacons, or similar technologies (collectively referred to as "Tracking Technologies") are used to help tailor our content, allow users to move between associated websites without logging into each site, and other purposes related to our management of Nick.com. Cookies are small text files stored locally on your machine that help store user preferences. "Web beacons" or "clear gifs" are small pieces of code placed on websites used to collect advertising metrics, such as counting page views, promotion views, or advertising responses.

We may use Tracking Technologies to understand site and Internet usage and to improve or customize the content, offerings or advertisements on Nick.com. For example, we may use cookies to personalize your experience on the Nick.com (e.g., to recognize you by name when

you return to a site), save your password in password-protected areas, save your online game or video player settings, and enable you to use shopping carts on the site. We also may use cookies to help us offer you products, programs, or services that may be of interest to you and to deliver relevant advertising. By agreeing to this Privacy Policy, you are consenting to the use of Tracking Technologies as set forth in this Policy. This Site adheres to the Self-Regulatory Principles for Online Behavioral Advertising. Click here for more information about this Site and online behavioral advertising.

…

Nick.com may additionally use a variety of third party advertising networks, data exchanges, traffic measurement service providers, marketing analytics service providers and other third parties (collectively, "Third Party Advertising Service Providers") to, for example, serve advertisements on Nick.com, facilitate targeting of advertisements and/or measure and analyze advertising effectiveness and/or traffic on Nick.com ("Targeting Services"). These Third Party Advertising Service Providers may enable us to display advertisements based on your visits to Nick.com and other websites you have visited. Targeting Services enable us to, among other things, help deliver advertisements or other content to you for products and services that you might be interested in, to prevent you from seeing the same advertisements too many times and to conduct research regarding the usefulness of certain advertisements to you.

Although these Third Party Advertising Service Providers do not have access to Tracking Technologies set by Nick.com, the Third Party Advertising Service Providers, as well as advertisers, may themselves set and access their own Tracking Technologies and/or they may otherwise have access to information about you.

http://corporate.disney.go.com/corporate/pp_online-tracking-advertising.html

Examples of online tracking technologies include:

> Cookies. Cookies are pieces of information that a website places on the hard drive of your computer when you visit the website. Cookies may involve the transmission of information from us to you and from you directly to us, to another party on our behalf, or to another party in accordance with its privacy policy. We may use cookies to bring together information we collect about you. You can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies. You do this through your browser settings. Each browser is a little different, so look at your browser Help menu to learn the correct way to modify your cookies. If you turn cookies off, you won't have access to many features that make your guest experience more efficient and some of our services will not function properly.
>
> Flash cookies. We may use local shared objects, sometimes known as Flash cookies, to store your preferences or display content based upon what you view on our site to personalize your visit. Our advertisers and third-party service providers also may use Flash cookies to collect and store information. Flash cookies are different from browser cookies because of

the amount of, type of, and how data is stored. Cookie management tools provided by your browser will not remove Flash cookies. To learn how to manage privacy and storage settings for Flash cookies, please click here. If you disable Flash cookies, you won't have access to many features that make your guest experience more efficient and some of our services will not function properly.

Web beacons. Web beacons are small pieces of data that are embedded in images on the pages of sites. Web beacons may involve the transmission of information directly to us, to another party on our behalf, or to another party in accordance with its privacy policy. We may use web beacons to bring together information we collect about you.

http://corporate.mattel.com/privacy-policy.aspx

How Does Mattel Use Cookies?

Mattel receives and stores certain information automatically whenever your visit our sites. Examples of information we collect and analyze include the Internet Protocol (IP) address used to connect your computer to the Internet; computer and connection information such as browser type and version; the operating system and platform you use; and pages viewed and time spent on our sites. This information helps us to optimize your experience at our sites. We also use cookies and clear GIFs, sometimes known as pixel tags or web beacons. Certain Internet Service Providers may assign the same IP address to many users. Your IP address and cookies are not connected to any personally identifiable or online contact information, like a name and address, unless you register or order at our online stores; however, if you register at our online stores, all information we collect will be associated with your customer file.

A "cookie" is a small file that is saved on your computer's hard drive which contains non-personal information. Our cookies help us improve your online experience, allow you to personalize your pages, enable us to customize our offerings, and help you to participate in some activities or events on our sites. For instance, we use cookies to keep track of your progress in certain games. If you leave a site and then return, cookies may allow you to continue the game so that you do not have to start all over again. Cookies keep track of items in your shopping cart and wish list in our online stores. Cookies help us determine how many people visit our sites, which of our web pages they use, and how long they stay there. This information helps us evaluate which of our web features are successes and which need improvement. You can disable the use of cookies through your Internet browser. Check your browser's Help menu to find out how. However, if you disable cookies you may not be able to take advantage of some features on our sites. Clear GIFs allow us to count the number of visitors viewing our pages, and in promotional emails they can tell us when the email has been opened.

7. Does Mattel Ever Collect Information Without Consent?

Mattel does not collect information passively through cookies or other tracking mechanisms

except in the circumstances described above. However, third-party advertisers may, so please review section 8 below. Mattel cookies DON'T contain any personal information about a specific user. We don't use cookies or other non-consensual methods to take personally identifiable or online contact information about you or your family off of your computer. Except for certain activities like scavenger hunts, which we talked about above, Mattel doesn't use cookies for direct marketing or promotional purposes. Mattel does not use cookies to collect information specifically about you or your family for sharing with third parties.

8. Do Mattel's Third-Party Advertisers Use Cookies?

At our adult areas, like our online stores, we may work with third-party network advertisers who use cookies, pixels, or transparent GIF files to help manage online advertising. These GIF files enable them to recognize a unique cookie on your Web browser. The cookie may be placed at our website or at another website who works with our third-party advertiser, and allows collection of information about your visits to our websites and to other websites that are part of the network. We also transmit certain information about your site visit to our third-party network advertiser. The information collected and shared in this fashion is anonymous. It does not contain your name, address, telephone number, or email address. It does identify possible interests in certain categories of products and services based upon your online activities. This information may be used for the purpose of targeting advertisements on this and other sites based on those interests, and to learn which ads bring users to our websites. For more information about our network advertisers, including information about how to opt out of receiving interest-based advertising through technologies that they control, click here. Please remember that we do not control the privacy policies and practices of any third party.

CHILDREN'S ONLINE PRIVACY POLICIES

AN ANALYSIS OF THE TOP CHILDREN'S WEBSITES

A RESEARCH STUDY

BY SHARON GOOTT NISSIM

DECEMBER 2011

ON BEHALF OF:

THE CENTER FOR DIGITAL DEMOCRACY

THE GEORGETOWN UNIVERSITY LAW CENTER INSTITUTE FOR PUBLIC REPRESENTATION,

FIRST AMENDMENT AND MEDIA LAW PROJECT[1]

[1] Prepared for inclusion as an appendix accompanying comments of Center for Digital Democracy, et al. on the Federal Trade Commission's proposal to amend the Children's Privacy Protection Rule to Respond to Changes in Online Technology. 76 Fed. Reg. 59804 (Sept. 29, 2011) (to be codified at 16 C.F.R. pt. 312).

AUTHOR BIOGRAPHY

Sharon Goott Nissim, J.D., is an expert in consumer privacy issues, including online tracking and behaviorally targeted advertising. Ms. Nissim graduated cum laude from Northwestern University School of Law in 2010 and received her B.A. with distinction in political science from Yale University in 2006. From 2010-2011 she was the Consumer Protection fellow at the Electronic Privacy Information Center, where her work focused on representing consumers' privacy interest before Congress, in the courts, and before federal regulatory agencies. Ms. Nissim has addressed privacy and public policy issues at leading conferences, including the Consumer Federation of America Annual Assembly and International Academy of Privacy Professionals Privacy Academy.

Ms. Nissim's article, A *Vicious Cycle: The Problem With Employer Credit Checks and Strategies to Limit Their Use*, was published in the fall 2010 edition of the Georgetown Journal on Poverty Law and Policy. She has clerked at the Midwest Center for Justice in Chicago, the Lawyers' Committee for Civil Rights in Washington, D.C., and the Civil Rights Division of the Illinois Attorney General's Office. She is a member of the Illinois Bar.

INTRODUCTION AND METHODOLOGY

The purpose of this study was to examine the privacy policies of the most popular children's websites to determine whether they comply with the FTC's rule implementing the Children's Online Privacy Protection Act (COPPA Rule).[2]

The privacy policies examined for this report were provided by the Center for Digital Democracy and the Institute for Public Representation at Georgetown. The policies were selected from a comScore list of the top 50 child- oriented companies most popular online among U.S. children ages 2-11.[3] The dataset included the privacy policy of at least one website from each top company that operates at least one site with a non-foreign top-level domain. For companies in control of several child-oriented websites, the privacy policies of multiple sites were examined and, if found to differ materially from each other, were included separately in the dataset. The privacy policies examined for this report are meant to closely approximate, but not exhaustively

[2] 16 C.F.R. §312, Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,899 (Nov. 3, 1999); see also Children's Online Privacy Protection Act, 15 U.S.C. §6501, et seq.

[3] For details on the comScore list, see the accompanying filing to the FTC.

comprise, the privacy policies of the 50 child-targeted companies most popular among U.S. children online. The statistics in this report are rounded to the nearest whole number.

The research focused on several key questions:

- **WERE THE PRIVACY POLICIES EASY TO FIND?**
- **DID THE SITES HAVE SEPARATE PRIVACY POLICIES FOR CHILDREN?**
- **WHAT PERSONALLY IDENTIFYING INFORMATION (PII) DID THE COMPANIES ADMIT TO COLLECTING FROM CHILDREN?**
- **WHAT OTHER INFORMATION DID THE COMPANIES ADMIT TO COLLECTING IN THEIR POLICIES?**
- **WHAT KIND OF PASSIVE TRACKING OF THEIR USERS DID THE SITES ADMIT TO?**
- **WITH WHAT ENTITIES DO THE COMPANIES SHARE THE INFORMATION THEY COLLECT AND FOR WHAT PURPOSE?**
- **WHAT, IF ANY, MECHANISM FOR OBTAINING PARENTAL CONSENT OR GIVING NOTIFICATION TO PARENTS WHEN CHILDREN'S INFORMATION IS COLLECTED WAS DESCRIBED IN THE POLICIES?**
- **DO THE COMPANIES ADMIT TO ENGAGING IN BEHAVIORALLY TARGETED ADVERTISING, OR ALLOWING THIRD-PARTIES TO DO SO? ARE THESE THIRD-PARTIES NAMED?**
- **ARE THE POLICIES OVERALL CONFUSING FOR A PARENT? ARE THERE ANY LOOPHOLES OR INTERNAL CONTRADICTIONS?**

FINDINGS

The majority of websites are out of compliance with some aspect of the current version of the COPPA Rule. Following are some of the most significant findings of this research:

- **81% OF THE TOP SITES HAVE LINKS TO THEIR PRIVACY POLICIES THAT ARE IN SMALLER THAN 10-POINT FONT.**[4]

[4] This was done by copying and pasting the privacy policy link into a word document to determine the font size.

- **OVER THREE-QUARTERS OF THE TOP CHILDREN'S SITES ALLOW FOR THE COLLECTION OF SOME TYPE OF PERSONAL INFORMATION FROM CHILDREN**
- **HALF OF THOSE SITES REQUIRE PARENTAL CONSENT, AND 34% OF THOSE SITES ONLY PROVIDE FOR PARENTAL NOTIFICATION.**
- **73% OF SITES MENTION THE USE OF SOME FORM OF TRACKING TECHNOLOGY IN THEIR PRIVACY POLICY**
- **64% OF THE TOP SITES EXPLICITLY ADMIT TO SOME FORM OF BEHAVIORALLY TARGETED ADVERTISING.**

In addition to the variables above that are easy to quantify, another way in which the sites do not comply is that many of them are clearly too complex for the average parent to understand. Complexity is difficult to measure, but given the time it took an experienced privacy attorney to review and understand these policies, it is likely that most parents and non-privacy legal professionals would find them difficult to comprehend. Most of the policies did not come close to being "clearly and understandably written," as the COPPA Rule requires.[5] They are also often difficult to find, as outlined in the "Placement of Privacy Policy" section below.

One of the most striking findings was how children's privacy policies are structured. The policies often contain blanket general "privacy-friendly" statements up-front (i.e. "we never collect PII from children" or "we never share personal information with third parties"), and then follow those statements with detailed exceptions. The policies appear to be, in many cases, intentionally designed if not to mislead, then at least to confuse and to give parents a false sense of comfort.

Most of the policies have a section within the general policy that specifically addresses children's privacy, as opposed to an entirely separate policy. The children's section generally comes towards the end of the privacy policy page, and often appears to contradict much of what came before it. Even if legally it may supersede the general policy, few parents are likely to understand that.

Additionally, many privacy policies suggest that operators do not always require parental consent when they should. For example, some privacy policies indicate that operators will merely notify parents after they collect personal information, rather than obtaining parental consent before collecting the information. A significant number of privacy policies also

[5] 16 C.F.R. § 312.4 (b)(1)(ii).

potentially allow operators to collect a child's first name and e-mail with neither parental consent nor notification.

Lastly, the way in which the sites address behaviorally targeted advertising is particularly misleading, as they often disavow engaging in the practice, but then admit that third parties may do so, but assert that those third parties are not covered under the privacy policy. The privacy policies of these third-parties are rarely made available.

RESULTS

PLACEMENT OF PRIVACY POLICY

Under the COPPA Rule, a privacy notice is required for every website directed to children, and a link to the required privacy notice must be placed in a "clear and prominent manner" on the homepage of the website.[6] Yet, most of the websites in this study violated this aspect of the law. **81% of the top sites have links to their privacy policies that are in smaller than 10-point font.**[7] On many of these sites the link is buried in a homepage that is full of text and is certainly not "clear and prominent."

In the majority of sites, one section of the main privacy policy is devoted to dealing with the subject of children's privacy.[8] In two cases, however, users have to click on more than one link to get to a children's privacy policy that is separate from the main privacy policy.[9]

"CLEARLY AND UNDERSTANDABLY"

Under the COPPA Rule, all privacy notices must be **"clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory material."**[10]

---

[6] 16 C.F.R. § 312.4 (b)(1)(ii).

[7] This was done by copying and pasting the privacy policy link into a word document to determine the font size.

[8] *See, e.g.,* Ganz World Privacy Policy, *available at* http://www.ganzworld.com/privacy-policy/; 4Kids Privacy Policy, *available at* http://www.4kids.tv/information/privacy-policy; Sesame Street Privacy Policy, *available at* http://www.sesamestreet.org/privacypolicy.

[9] StarFall, *available at* http://www.starfall.com/n/N-info/helpdesk.htm#privacy; WebKinz, *available at* http://www.webkinz.com/us_en/privacy_policy.html.

[10] 16 C.F.R. §312.4(a).

Below are a few emblematic examples from the top websites' privacy policies of language that is unclear, difficult to understand, and often internally contradictory. In particular, many sites have separate sections for children's privacy within their more general privacy policy, but it would not be obvious to the average reader whether the policies described in the children's privacy section supersede the other general, and often contradictory, policies.

> *"Please know that certain areas and features of Nick.com only can be accessed in conjunction with cookies or similar devices and you should be aware that disabling cookies or similar devices might prevent you from accessing some of our content. . . Nick.com may additionally use a variety of third party advertising networks, data exchanges, traffic measurement service providers, marketing analytics service providers and other third parties . . . to, for example, serve advertisements on Nick.com, facilitate targeting of advertisements and/or measure and analyze advertising effectiveness and/or traffic on Nick.com."*[11]
>
> *"The Third Party Advertising Service Providers, as well as advertisers, may themselves set and access their own Tracking Technologies and/or they may otherwise have access to information about you. . . You should be aware that different rules might apply to the collection, use or disclosure of your information by third parties in connection with their advertisements, promotions and other websites you encounter on the Internet."*[12]

> *A member of The Walt Disney Family of Companies, which includes many different brands, will be the data controller for your information . . . Other members of The Walt Disney Family of Companies may have access to your information where they perform services on behalf of the data controller(s) (as a data processor) and, unless prohibited under applicable law, for use on their own behalf (as a data controller) for the following purposes . . .* [13]

[11] Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html.

[12] *Id.*

[13] Disney Privacy Policy, *available at* http://corporate.disney.go.com/corporate/pp.html.

> *This is the official privacy policy ("Privacy Policy") for the Flux platform ("Flux," "we," "us," or "our"), an online social-networking and social-media service, and the Flux web sites located at www.Flux.com and www.socialproject.com (the "Flux Sites"). Flux and Flux Sites are offered by Social Project Inc. ("Social Project"). Social Project is an MTV Networks ("MTVN") Company. MTVN is a division of Viacom International Inc. (together with MTVN, the "Parent Companies"). Using Flux, also we power and host certain portions of web sites owned by the Parent Companies or third parties ("Third Party Sites"). The Flux Sites and Third Party Sites make up a community of social-networking web sites that we refer to here as the "Community Sites." The Community Sites, using Flux, allow registered users of the Community Sites ("Members") to create personal profiles online, display content, share information and comments, and establish a network of relationships – all within one Community Site or across multiple Community Sites.*[14]

> *"Otherwise, personal information will be collected, used and disclosed in accordance with the form of consent required by applicable law and its use will be limited to the objectives for which it was collected as described herein. The form of your consent can vary from implied consent to express consent, depending on the circumstances and sensitivity of the information collected."*[15]

> *"At some places on the Site, we may ask your permission to disclose personally identifiable information about you to companies whose practices are not covered by this Privacy Policy . . . that want to market products or services to you. If at some point you grant us permission to transfer your information for these purposes and later decide that you no longer want us to do so, simply log into your profile if you have created an account with us, or send us an email . . . we will edit your preferences accordingly . . . We may, on occasion, combine information we receive online with outside*

[14] Social Project Privacy Policy, *available at* http://www.socialproject.com/PrivacyPolicy.html [part of "Flux Network," referenced in Nick Jr. privacy policy.

[15] Ganz World Privacy Policy, *available at* http://www.ganzworld.com/privacy-policy/.

> *records to enhance our ability to market to you those products or services that may be of interest to you."*[16]

ACTIVE COLLECTION OF PERSONAL INFORMATION

The COPPA Rule forbids the collection, use, or disclosure of "personal information" from children without "verifiable parental consent," except in certain limited circumstances.[17] These limited circumstances include collecting contact information in order to obtain parental consent, to respond on a "one-time basis" to a child's request, to reply more than once to a specific request (only with parental notice), and to provide for the child's safety.[18]

The COPPA Rule defines one category of "collection" as "requesting that children submit personal information online." Many of the top sites request that a child submit information either to register to use certain parts of the site, or most often, to sign up for an electronic newsletter or a contest. Most sites offer a general disclaimer that they try to avoid collecting personal information from children, and that they never require more personal information than is reasonably necessary. Many also insist that they require parental permission for collecting personal information from children under 13. But what do the sites actually admit to doing in their privacy policies?

- **OVER THREE-QUARTERS OF THE TOP CHILDREN'S SITES ALLOW FOR THE COLLECTION OF SOME TYPE OF PERSONAL INFORMATION FROM CHILDREN.**[19]
- **HALF OF THE SITES THAT MAY COLLECT PERSONAL INFORMATION REQUIRE SOME FORM OF PARENTAL CONSENT IN ORDER TO DO SO.**[20]
- **34% OF SITES THAT MAY COLLECT PERSONAL INFORMATION ONLY PROVIDE FOR PARENTAL NOTIFICATION, NOT CONSENT.**[21]

---

[16] DC Comics Privacy Policy, *available at* http://dccomics.com/dccomics/legal/?action=privacy.

[17] 16 C.F.R. §312.3.

[18] *Id*. at §312.5(c).

[19] *See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Disney Privacy Policy, *available at*http://corporate.disney.go.com/corporate/pp.html; Cartoon Network Privacy Policy, *available at* http://www.cartoonnetwork.com/legal/privacy.html; Mattel Privacy Policy, *available at* http://corporate.mattel.com/privacy-policy.aspx.

[20] *See, e.g.,* Disney Privacy Policy, *available at*http://corporate.disney.go.com/corporate/pp.html; Marvel Kids Privacy Policy, *available at* http://marvelkids.marvel.com/privacy/; PBS Kids Privacy Policy, *available at* http://pbskids.org/privacy/index.html?campaign=fkhp_prv.

According to the COPPA Rule, personal information includes a child's first and last name, physical address, e-mail address, screen name that reveals an e-mail address, and telephone number.[22] Based on the privacy policies examined, that the most common personal information operators collect is a child's e-mail address, often combined with first name.

The language sites use to explain when parental consent or notification is required is often non-specific. In addition, many policies suggest that the operator collects information without consent, but will later delete the information upon request. Operators who do this presume consent is given until the parent affirmatively disapproves, rather than presuming consent is withheld until the parent affirmatively approves.[23] Following are some representative examples:

> *"With your verifiable consent, we may collect personal information from your child such as a last name, address or e-mail address when the information is necessary for a particular activity. If we need more than just your child's first name (or screen name) and e-mail address for your child to participate in a particular online activity, we will ask your child for your e-mail or mailing address so that we can notify you of your child's request and get your permission."*[24]

> *"Upon proper identification, parents may review the personal information we have collected online from their child, request deletion, or refuse to allow further collection or use by filling out a Parental Review Access Form and mailing it to the address on the form. However, if you ask us to delete your child's information from our marketing database, we may have to ask your child not to participate in our activities."*[25]

[21] *See, e.g., See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Cartoon Network Privacy Policy, *available at* http://www.cartoonnetwork.com/legal/privacy.html; American Girl Privacy Policy, *available at* http://store.americangirl.com/static/popups/privacyPolicy.html. [This statistic includes one site, WebKinz (http://www.webkinz.com/us_en/privacy_policy.html), which purports to use only the personal information for a one-time response, which would make mere notification acceptable under COPPA.]

[22] 16 C.F.R. §312.2 ("Definitions").

[23] Some sites do have specific and clear policies, for example: Cool Math (http://www.coolmath.com/privacyp.htm); PBS Kids (http://pbskids.org/privacy/index.html?campaign=fkhp_prv).

[24] Mattel Privacy Policy, *available at* http://corporate.mattel.com/privacy-policy.aspx.

[25] American Girl Privacy Policy, *available at* http://store.americangirl.com/static/popups/privacyPolicy.html.

> *"In cases where we have inadvertently collected personal information of a child, the parent can always review this information, choose to have this information deleted from our records and refuse to permit further collection or use of this information."*[26]

ACTIVE COLLECTION OF NON-PERSONAL INFORMATION

In addition to the "personal" information collected, most of the sites also collect several additional categories of information from children. Examples of information the sites deem "non-personal" include age, birthdate, gender, state or country, and sometimes zip code. Children are often asked to create a username and password, and often are urged to not use any personally identifying information in doing so.

However, research has shown that non-personal information can actually be used to personally identify an individual. A study by Latanya Sweeney, Ph.D., found that 87% of the U.S. population could potentially be identified based solely on 5-digit zip code, gender, and date of birth.[27] According to legal scholar Paul Ohm, "researchers have found data fingerprints in pools of non-PII data, with much greater ease than most would have predicted[, suggesting] that maybe everything is PII, to one who has access to the right outside information."[28]

- **22 SITES (41%) COLLECT BIRTHDAY INFORMATION FROM CHILDREN.**[29]
- **20 SITES (38%) COLLECT GENDER INFORMATION FROM CHILDREN.**[30]
- **18 SITES (34%) COLLECT STATE, COUNTRY, AND/OR TOWN INFORMATION FROM CHILDREN.**[31]

---

[26] Tower Hobbies Privacy Policy, *available at* http://www.towerhobbies.com/help/privacy.html.

[27] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely,* Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh 2000, *available at* http://dataprivacylab.org/projects/identifiability/paper1.pdf.

[28] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization 4 (University of Colorado Law Legal Studies Research Paper No. 09-12, 2009), 21, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006..8, 11, 13, 14.

[29] *See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Disney Privacy Policy, *available at*http://corporate.disney.go.com/corporate/pp.html.

[30] *See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Fisher Price Privacy Policy, *available at* http://www.fisher-price.com/us/privacy.asp.

- **15 SITES (28%) COLLECT AGE INFORMATION FROM CHILDREN.**[32]
- **13 SITES (24%) COLLECT CHILDREN'S FIRST NAMES.**[33]
- **11 SITES (21%) ALLOW OR REQUIRE CHILDREN TO CREATE SCREEN NAMES/USER NAMES AND/OR PASSWORDS.**[34]
- **7 SITES (13%) COLLECT CHILDREN'S ZIP CODES.**[35]

PASSIVE COLLECTION OF PERSONAL INFORMATION

Beyond the collection of information that a child may actively provide, most of these sites are also engaged in "passive" information collection. The passive collection of information takes place behind the scenes and is therefore less likely to be known to the user. Passive collection refers to the tracking of users on sites using cookies, flash cookies, web beacons, and other similar technologies. These technologies are used to track a variety of different metrics, including: IP address, parts of web site viewed, traffic patterns/usage, and demographic information of users. They can also be used to serve targeted advertisements by the first party (the web site itself) and by third party ad servers (see "Behaviorally targeted advertising" section).

The COPPA Rule includes this type of tracking in its definition of impermissible "collection" of personal information from children.[36] But the Rule's definition of "personal information" encompasses information collected through passive tracking only if the information includes a "persistent identifier" associated with "individually identifiable information," and does not

[31] *See, e.g.,* American Girl Privacy Policy, *available at* http://store.americangirl.com/static/popups/privacyPolicy.html; PBS Kids Privacy Policy, *available at* http://pbskids.org/privacy/index.html?campaign=fkhp_prv.

[32] *See, e.g.,* Fantage Privacy Policy, *available at* http://play.fantage.com/privacy_policy.html; PBS Kids Privacy Policy, *available at* http://pbskids.org/privacy/index.html?campaign=fkhp_prv.

[33] *See, e.g.,* Nick Jr. Privacy Policy, *available at* http://www.nickjr.com/about/privacy-policy.htm; Sprout Privacy Policy, *available at* http://www.sproutonline.com/sprout/info/privacypolicy.aspx.

[34] *See, e.g.,* Disney Privacy Policy, *available at* http://corporate.disney.go.com/corporate/pp.html; 4Kids Privacy Policy, *available at* http://www.4kids.tv/information/privacy-policy.

[35] *See e.g.,* AOL Kids Privacy Policy, *available at* http://kids.aol.com/site-info/privacy-policy/; Yahoo Kids Privacy Policy, *available at* http://info.yahoo.com/privacy/us/yahoo/kids/.

[36] 16 C.F.R. §312.2 (c) (referring to "the passive tracking or use of any identifying code linked to an individual, such as a cookie").

consist merely of aggregated information.[37] The Federal Trade Commission included "persistent identifiers" as covered information in its settlement agreements with Google and Facebook.[38]

- **73% OF SITES MENTION THE USE OF SOME FORM OF TRACKING TECHNOLOGY IN THEIR PRIVACY POLICY.[39]**
- **OF THOSE SITES, ONLY 29% EXPLICITLY STATE THAT THEY DO NOT COLLECT PERSONAL INFORMATION THROUGH THESE TRACKING TECHNOLOGIES.[40]**

SHARING OF PERSONAL INFORMATION

The COPPA Rule forbids the sharing or disclosing of children's information in "identifiable form" with third parties without verifiable parental consent of the highest form.[41] Accordingly, many of the top sites do specifically state that if they share children's information with third parties, it is either only for supporting the services of the site, or it is in aggregate form. But the user is forced to rely on the company's claims that the shared information is aggregate, de-identified, or not personally identifiable. The policies do not explain exactly what is shared and with whom, or whether this information could be used to re-identify an individual. The Federal Trade Commission (FTC), in its report on behavioral targeted advertising, noted that, "the line separating PII and non-PII has become increasingly indistinct."[42]

[37] 16 C.F.R. §312.2 (f).

[38] Federal Trade Commission, *In The Matter of Google, Inc.,* Decision and Order, Definitions §2(5), October 13, 2011, *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; Federal Trade Commission, *In The Matter of Facebook, Inc.,* Agreement Containing Consent Order, Definitions §4, November 29, 2011, *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

[39] *See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Disney Privacy Policy, *available at*http://corporate.disney.go.com/corporate/pp.html.

[40] *See, e.g.,* PBS Kids Play Privacy Policy, *available at* http://www.pbskidsplay.org/privacy; Fantage Privacy Policy, *available at* http://play.fantage.com/privacy_policy.html. [Two additional sites say they do not collect PII through these technologies but they may link information collected passively to personal information collected actively.]

[41] 16 C.F.R. §312.2 (a) (excepting for those third parties providing "support for the internal operations of the website").

[42] Federal Trade Commission Staff Report, "Self-Regulatory Principles for Online Behavioral Advertising," 32, February 2009, *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

- **30% OF SITES ALLOW THE SHARING OF CHILDREN'S INFORMATION WITH THIRD PARTIES, BUT ONLY IN AGGREGATED (OR NON-PERSONALLY IDENTIFIABLE) FORM.[43]**
- **11% ALLOW SHARING OF INFORMATION WITHIN THE "FAMILY" OF COMPANIES OR WITH AFFILIATES.[44]**
- **21% EXPLICITLY STATE THAT THEY DO NOT SHARE CHILDREN'S INFORMATION WITH THIRD PARTIES (BUT MAY DO SO WITH AN ADULT'S INFORMATION).[45]**

BEHAVIORALLY TARGETED ADVERTISING

One of the reasons that websites collect information from tracking technologies (as outlined in the "passive collection" section) is to serve targeted advertisements to the user. While the COPPA Rule does not directly address behaviorally targeted advertising,[46] the fast-changing practices in this area call for a renewed focus on this issue. Many of the top sites engage in behaviorally targeted advertising.

- **64% OF THE TOP SITES EXPLICITLY ADMIT TO SOME FORM OF BEHAVIORALLY TARGETED ADVERTISING.[47]**
- **OF THOSE SITES, 65% ADMIT TO DOING THE TARGETING THEMSELVES, USING THEIR OWN TRACKING TECHNOLOGIES[48] AND 68% ADMIT TO ALLOWING THIRD PARTIES TO TRACK USERS AND DO TARGETED ADVERTISING.[49]**

---

[43] *See, e.g.,* AOL Kids Privacy Policy, *available at* http://kids.aol.com/site-info/privacy-policy/; National Geographic Kids Privacy Policy, *available at* http://kids.nationalgeographic.com/kids/policies/privacypolicykids/.

[44] *See, e.g.,* Disney Privacy Policy, *available at* http://corporate.disney.go.com/corporate/pp.html; Bratz Pack Privacy Policy, *available at* http://www.mgae.com/Privacy/privacyenglish.asp. In many cases, this opens up a large world of permissible sharing that most parents would not necessarily understand. For example, the Disney family includes the following companies, among others: ABC, Baby Einstein, BabyZone, Club Penguin, ESPN, Hollywood Records, Kaboose, Marvel, Muppets, Pixar, Playdom, Tapulous, Touchstone.

[45] *See, e.g.,* American Girl Privacy Policy, *available at* http://store.americangirl.com/static/popups/privacyPolicy.html; Barbie Privacy Policy, *available at* http://www.everythinggirl.com/common/policy.aspx?site=barbie.

[46] It addresses the sharing of personal information with third parties. The definition of personally identifying may encompass some of the information used for targeted advertising.

[47] *See, e.g.,* Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html; Disney Privacy Policy, *available at*http://corporate.disney.go.com/corporate/pp.html.

[48] *Id.*

- **ONLY 11% EXPLICITLY STATE THAT THEY DO NOT ENGAGE IN BEHAVIORALLY TARGETED ADVERTISING, AND 22% LEAVE THE POSSIBILITY OPEN.[50]**

The COPPA Rule does require companies to list all third-party operators that collect personal information on their sites, as well as detailed contact information for those operators.[51] **Only 10 sites (27% of sites that allow third-party tracking and advertising) even named the third parties, and of those all but one named only Double Click, and just provided a link to more information.**

The sites vary in the language they use to explain behaviorally targeted advertising, although none actually call it that. The following are common examples:

> *Tracking technologies are used to "understand site and Internet usage and to improve or customize the content, offerings or advertisements on Nick.com."*[52]

> *"We use registration information to enable you to take advantage of site offerings, respond to your requests, for game management purposes, to serve appropriate material and to provide you with opportunities to learn of additional products or services that we believe may be of interest to you."*[53]

> *"We may on occasion combine information we collect through our Sites with information that we collect from other sources. We sometimes use non-personally identifiable information that we collect to improve the design and content of our Sites, and to improve our visitors' experience on the Sites.*

[49] *See, e.g.,* Marvel Kids Privacy Policy, *available at* http://marvelkids.marvel.com/privacy/*;* Cartoon Network Privacy Policy, *available at* http://www.cartoonnetwork.com/legal/privacy.html. [There is overlap here – some do both, some only first party or only third party.]

[50] The first and second bullet point statistics add up to 96% because of the two sites for which no privacy policy was available at all.

[51] 16 C.F.R. §312.4 (b)(2)(i).

[52] Nickelodeon Privacy Policy, *available at* http://www.nick.com/info/privacy-policy.html.

[53] Monkey Quest Privacy Policy, *available at* http://www.monkeyquest.com/en/privacy-policy. This is one of the rare companies that admits in its policy to using registration information for advertising purposes, as opposed to just information taken from passive tracking technologies.

> *We also may aggregate, use and share this information with third parties to analyze Site usage, as well as to offer products, programs, or services."*[54]

> *"We may obtain customer lists, demographic and other information from other sources. We may combine this information with information we collect online to better understand your needs, improve our site, our products, and our services, and better serve you."*[55]

CONCLUSION

The results demonstrate that many of the top children's websites' privacy policies and practices do not fully comply with the current version of the COPPA Rule. The majority of sites have links that are not easy to find, policies that are written in a confusing manner, and loopholes and contradictions that make them difficult for parents to understand. Many of the sites evidently collect information personal information from children without verifiable parental consent. Many websites that do not collect what they deem "personal information," still collect many pieces of "non-personal information" that could potentially be used to re-identify a child user.

The results also show that there is much more tracking going on behind the scenes. A significant majority of sites are using passive tracking technologies to collect information about a user, including persistent identifiers such as IP address. The sites are often using that information to serve behaviorally targeted advertising, or allowing third-parties to track users and provide those ads.

These findings reveal that as of now, it is difficult for a child to have a safe online experience and for a parent to understand exactly what information is being collected about his or her child.

[54] Cartoon Network Privacy Policy, *available at* http://www.cartoonnetwork.com/legal/privacy.html.

[55] American Girl Privacy Policy, *available at* http://store.americangirl.com/static/popups/privacyPolicy.html.