Report to the Maryland General Assembly on Children's Online Privacy

Workgroup on Children's Online Privacy Protection
Convened by the Maryland Office of the Attorney General
Baltimore, Maryland

December 30, 2013

Contributing Staff

Lead Writers
Stephen M. Ruckman
Steven M. Sakamoto-Wengel

Reviewers
Members of the Workgroup
Kisha A. Brown
Katherine Foster

Members of the Workgroup on Children's Online Privacy Protection

Angela Campbell
Co-Director, Institute for Public Representation
Georgetown University Law Center

Will Castleberry
Director, State and Local Public Policy
Facebook

Jerry Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association

Chris DiPietro
Consultant
Microsoft

Amina Fazlullah
Policy Counsel
Benton Foundation

David Jacobs
Consumer Protection Counsel
Electronic Privacy Information Center (EPIC)

Wayne Keeley
Director
CBBB's Children's Advertising Review Unit

Sara Kloek
Director of Outreach
Association for Competitive Technology

Allison Lefrak
Attorney, Division of Privacy and Identity Protection
Federal Trade Commission

Joni Lupovitz
Vice President, Policy
Common Sense Media

Doug Miller
Global Privacy Leader
AOL

Paula Minsk
Executive Director
American Academy of Pediatrics – Md. Chapter

Kathryn Montgomery
Professor, School of Communication
American University

Emma Morris
International Policy Manager
Family Online Safety Institute

Stephen M. Ruckman, *Co-Chair*
Assistant Attorney General &
Director, Internet Privacy Unit
Maryland Office of the Attorney General

Steven M. Sakamoto-Wengel, *Co-Chair*
Assistant Attorney General
Maryland Office of the Attorney General

Vans Stevenson
Senior Vice President for State Government Affairs
MPAA

Marceline White
Executive Director
Maryland Consumer Rights Coalition

This report is available online at: http://www.oag.state.md.us/Reports/COPW.pdf

Transmittal Letter

DOUGLAS F. GANSLER
Attorney General

KATHERINE WINFREE
Chief Deputy Attorney General

JOHN B. HOWARD, JR.
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

410-576-7036
FACSIMILE NO.

410-576-6311
WRITER'S DIRECT DIAL NO.

December 30, 2013

The Honorable Thomas V. Mike Miller, Jr.
President of the Senate
State House
Annapolis, Maryland 21401

The Honorable Michael E. Busch
Speaker of the House of Delegates
State House
Annapolis, Maryland 21401

The Honorable Thomas M. Middleton
Chair, Senate Finance Committee
Miller Senate Office Building, 3East Wing
11 Bladen Street
Annapolis, Maryland 21401

The Honorable Dereck E. Davis
Chair, House Economic Matters Committee
House Office Building, Room 231
6 Bladen Street
Annapolis, Maryland 21401

Re: Report of the Children's Online Privacy Workgroup
MSAR # 9833; Citation: SB 374/Ch. 246, 2013

Dear President Miller, Speaker Busch, Chairman Middleton and Chairman Davis:

Chapter 246 (Senate Bill 374) of the 2013 General Assembly established the Workgroup on Children's Online Privacy Protection, which was tasked with examining issues relating to the protection of children's privacy while using the Internet and mobile applications and submitting a report offering its findings and any resulting recommendations by the end of 2013. On behalf of the Attorney General Doug Gansler, we respectfully submit the final report.

This report is intended to equip the General Assembly to make informed choices about how it wants to work toward strong, sensible protections for children's privacy on the Internet. While several proposed recommendations made to the Workgroup are included in this report, their inclusion should not be interpreted as an endorsement by the Workgroup. They are shared in the interest of making available to the General Assembly all ideas and materials made available to the Workgroup's members. We hope you find the report to be of assistance.

Sincerely,

Stephen M. Ruckman
Assistant Attorney General &
Director, Internet Privacy Unit

Steven M. Sakamoto-Wengel
Consumer Protection Counsel for
Regulation, Legislation and Policy

cc: Members of the Senate Finance Committee
Members of the House Economic Matters Committee

Contents

Introduction

Children's online privacy has been an important issue since the early days of the Internet. In the mid-1990s, when Internet usage was beginning to become more common in U.S. households, parents discovered that collection and sale of personal information about their children was becoming more common as well. Investigative reports revealed that major marketing firms were selling phone numbers and addresses of families with children without oversight as to how that personal information was being shared and with whom, causing that information to become readily available to child predators and others lacking concern for children's welfare.[1]

In April of 1998, the Federal Trade Commission ("FTC") issued a report to Congress on online privacy that found that children were "a large and rapidly growing segment of online consumers and are being actively targeted by commercial Web sites" because of their growing amount of market influence.[2] The FTC expressed concern that "[a] wide variety of detailed personal information is being collected online from and about children, often without actual notice to or an opportunity for control by parents," noting that 89% of commercial websites it surveyed collected personal information from children, with less than 10% offering parental controls.[3] It also expressed concern that children are particularly vulnerable to information collection by third parties, given that they "generally lack the developmental capacity and judgment to give meaningful consent to the release of personal information to a third party," and given their uncritical willingness to respond to incentives for providing personal information, such as entry into a contest, membership in a club, or access to a game.[4]

Concerns over collection of personal information about children eventually led Congress to pass the Children's Online Privacy Protection Act ("COPPA")[5] in October 1998. COPPA was designed to provide notice to consumers about online information collection practices, limit the collection of personal information from children online without parental consent, and maintain the confidentiality and security of any information collected.[6]

While COPPA laid a solid foundation of protections, the intervening 15 years have seen dramatic changes in Internet use and technology that warrant renewed focus on how best to protect children's privacy online. When COPPA was passed in 1998, only about a quarter (26.2%) of U.S. households had Internet access,[7] and only approximately 4.1% of children ages

---

[1] *Largest database marketing firm sends phone numbers, addresses of 5,000 families with kids to TV reporter using name of child killer*, BUSINESS WIRE, May 13, 1996, *available at*: http://epic.org/privacy/kids/KCBS_News.html.

[2] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO Congress 4 (1998), *available at*: http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a.pdf.

[3] *Id*. at 5 & 31-37.

[4] *Id.* at 6; *see id.* ("In sum, the immediacy and ease with which personal information can be collected from children online, combined with the limited capacity of children to understand fully the potentially serious safety and privacy implications of providing that information, have created deep concerns about current information practices involving children online.").

[5] 15 U.S.C. §§ 6501-6506.

[6] FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 5 (1999).

[7] U.S. CENSUS BUREAU, HOME COMPUTERS AND INTERNET USE IN THE UNITED STATES: AUG. 2000 1, Fig. 1 (Sept. 2001) ["2000 CENSUS REPORT"].

3-4, 16.8% of children ages 5-9, and 39.2% of children ages 10-13 used the Internet.[8] Today, over 70% of U.S. households have Internet access,[9] and 30% of children ages 3-5 and 50% of children ages 6-9 use the Internet on a typical day, with the percentage rising the older a child gets (67% usage by age 8).[10]

In addition to greater access to and use of the Internet, new Internet-connected technologies – from smart phones to Wi-fi-enabled cameras to e-readers and tablet computers – are proliferating in ways that increase children's exposure to the Internet. Indeed, there are many Wi-fi-enabled "kids tablets" on the market,[11] and hundreds, if not thousands, of online applications ("apps") directed at children and teens can be accessed by them on parents' phones and other mobile devices. Social media apps, in particular, are becoming part of everyday life for many children and a key portal through which they share information with their friends and start to form their own identity.[12] Recent research has shown that almost twice as many children are using mobile media now as there were just two years ago, and "the average amount of time children spend using mobile devices has tripled."[13] "In fact, today, 38% of toddlers *under 2* have used a mobile device" or mobile media in the past year.[14]

Children's enhanced Internet access and exposure to Internet-connected technology is wonderful when used to expand their education and support their development, but it is also risky in that it increases the potential for children's personal information to be collected and made widely available. It is also potentially confusing for children, who lack the cognitive ability to differentiate among forms of media content, e.g. the difference between advertising and non-advertising content.[15] As the Internet and Internet-connected devices become more entwined in the lives of children, more attention must be paid to how to best ensure that children, with the help of their parents or guardians, can navigate the Internet safely and knowledgeably, without putting their personal information at risk. The Workgroup on Children's Online Privacy Protection, convened by the Office of the Attorney General at the direction of the General Assembly, urges that more attention be given to these critical issues.

---

[8] NTIA, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET 43 (2002), *available at*: http://www.ntia.doc.gov/legacy/ntiahome/dn/anationonline2.pdf; *see also* 2000 CENSUS REPORT 4, Table B (showing that 7.3% of children ages 3-5 and 24.7% of children ages 6-11 used the Internet at home in 2000).

[9] U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES 2, Fig. 1 (May 2013).

[10] AVIVA LUCAS GUTNICK ET AL., SESAME WORKSHOP, ALWAYS CONNECTED: THE NEW DIGITAL MEDIA HABITS OF YOUNG CHILDREN 16 & 30 (2011), *available at*: http://www.joanganzcooneycenter.org/wp-content/uploads/2011/03/jgcc_alwaysconnected.pdf; *see also* DONELL HOLLOWAY ET AL., ZERO TO EIGHT: YOUNG CHILDREN AND THEIR INTERNET USE 8 (2013), *available at*: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf ("In the US, 25% of 3 year olds go online daily, rising to about 50% by age 5 and nearly 70% by age 8.")

[11] *See, e.g.*, http://www.toysrus.com/family/index.jsp?categoryId=19948766

[12] PEW RESEARCH CENTER'S INTERNET & AMERICAN LIFE PROJECT, TEENS, SOCIAL MEDIA, AND PRIVACY 2 (May 2013), *available at*: http://pewinternet.org/~/media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy.pdf.

[13] COMMON SENSE MEDIA, ZERO TO EIGHT: CHILDREN'S MEDIA USE IN AMERICA 2013 9 (2013), *available at*: http://www.commonsensemedia.org/sites/default/files/research/zero-to-eight-2013.pdf.

[14] *Id.*

[15] *See, e.g.*, Samantha Graff, Dale Kunkel & Seth E. Mermin, *Government Can Regulate Food Advertising to Children Because Cognitive Research Shows that it is Inherently Misleading*, 31 HEALTH AFFAIRS 2 392-398 (2012) ("Cognitive research indicates that young children cannot effectively recognize the persuasive intent of advertising or apply the critical evaluation required to comprehend commercial messages.").

Workgroup on Children's Online Privacy Protection: Background and Process

The Workgroup on Children's Online Privacy Protection (hereinafter "Children's Online Privacy Workgroup" or "Workgroup") was created by statute signed on May 2, 2013.[16] The law required the Office of the Attorney General ("OAG") to convene and direct a Workgroup to examine six key issues relating to the protection of children's online privacy:

(1) the nature and extent of data collected about children through Internet–based and mobile application–based advertising ("online advertising");

(2) current and forthcoming federal and state regulation of children's online privacy and online advertising and associated data collection;

(3) the effects on children of online behavioral advertising, native advertising, social advertising, and other forms of online advertising;

(4) best practices used by the Internet industry and the mobile application industry to protect children's online privacy;

(5) best practices urged by consumer advocates, children's health advocates, and regulators to protect children's online privacy; and

(6) the effectiveness of voluntary standards as they relate to children's online privacy.

The law required that a report on "the findings of the Workgroup and any resulting recommendations" be submitted to the Senate Finance Committee and House Economic Matters Committee by December 31, 2013.

This Workgroup was required to include among its members "representatives of State government, industry leaders, members of the academic community studying children's online privacy and the effects of online advertising on children, consumer advocates, and children's health advocates." The OAG convened an 18-member Workgroup that comprised two members of state government; one member of the FTC, the federal government agency that monitors online privacy; seven industry leaders, including high-level representatives from AOL, Facebook, Microsoft, the Council of Better Business Bureaus, and online advertising associations; six consumer advocates, composed of representatives from the Benton Foundation, Common Sense Media, the Electronic Privacy Information Center, the Family Online Safety Institute, Georgetown University Law Center's Institute for Public Representation (which includes among its clients the Center for Democracy and Technology), and the Maryland Consumer Rights Coalition; a leading professor studying children in the digital age; and the Executive Director of the Maryland Chapter of the American Academy of Pediatrics. A full listing of the Workgroup membership is listed on p. ii of this report. Because the Workgroup was designed to include a range of diverse and even opposing views in its membership, the material in this report does not always reflect the views of all Workgroup members.

[16] 2013 Md. Laws, Ch. 246. See Appendix A for the full text of the law.

The legislation establishing the Workgroup became effective on June 1, 2013, and the Workgroup began its study of children's online privacy soon thereafter, holding its first meeting on June 25, 2013. Meetings were generally held on a monthly basis throughout the remainder of 2013, with the final meeting occurring on December 16, 2013.

To ensure close review of the six issues the General Assembly required it to examine, the Workgroup identified research liaisons for each issue area, who coordinated research and reported on their findings at Workgroup meetings. The Workgroup also opened a public comment account, childrensprivacy@oag.state.md.us, advertised on the OAG website, to collect comments from interested parties on matters relevant to the Workgroup's study.

The Workgroup drew on the information it learned in each of the six issue areas to then discuss proposed recommendations to the General Assembly regarding how Maryland can improve protections for children's online privacy. Early in the process, the Workgroup decided that it would not put forward a formal list of recommendations that were submitted to an up-or-down vote, but would rather report to the General Assembly all recommendations proposed by Workgroup members and discussed by the full Workgroup, reflecting the range of views held by various members on each proposal, and noting the objections that were raised.

It is the intent of the Workgroup not to prescribe particular legislative outcomes, but rather to equip the General Assembly to make informed choices about how it wants to work toward strong, sensible protections for children's privacy on the Internet. While several proposed recommendations made to the Workgroup are included in this report, their inclusion should not be interpreted as an endorsement by the Workgroup. They are shared in the interest of making available to the General Assembly all ideas and materials made available to the Workgroup's members.

Workgroup Findings

Below are the findings presented to the Workgroup over the course of its term on each of the six issues the Workgroup was tasked with reviewing. These findings are descriptive, rather than prescriptive.

Issue 1: The Nature and Extent of Data Collected about Children through Internet–Based and Mobile Application–Based Advertising ("Online Advertising")

Online Data Collection about Children Has Been Extensive

The Workgroup learned that online data collection about children has been extensive, at least up until the FTC's updated COPPA Rule took effect in July 2013. A 2010 *Wall Street Journal* investigation found that websites popular among children and teens installed more data-gathering technology on computers than websites aimed at adults.[17] The investigators found 4,123 cookies, beacons, and other tracking tools installed on a test computer that visited the top 50 U.S. sites popular with children and teens, 30% more than the tracking tools found in an analysis of the top 50 U.S. sites overall, which are generally aimed at adults.[18] Some websites and apps that are aimed at a mixed audience that includes both teens and adults, like some popular photo-sharing websites and apps, are also popular among pre-teens and younger children, creating additional channels of data collection.[19]

The Workgroup learned that data about children is collected by child-oriented websites and apps and also the third-party advertisers that appear on them. Some of this data collection is done behind the scenes, through the placement of tracking cookies, beacons, and other persistent identifiers. Some of it is done through the actions of children themselves. For example, children are drawn to online "advergames" – games designed by or for advertisers to build interest in their products or brand – and they often input information about themselves into these advergames, like their name and their product preferences.[20] And recent research presented to the Workgroup shows that 53% of teens ages 14-17 have posted their email address online through social media sites, 71% have posted the city or town in which they live, and 91% have posted photos of themselves.[21]

---

[17] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, WALL ST. J., Sept. 17, 2010, *available at*: http://online.wsj.com/news/articles/SB10001424052748703904304575497903523187146.

[18] *Id.* Workgroup member Direct Marketing Association stressed that the Workgroup should not rely on the *Wall Street Journal* findings because they address sites popular with children *and teens*, and the Workgroup's focus is on children. Also, the sites analyzed by the *Wall Street Journal* complied with the then-applicable COPPA Rule, according to the article's authors, so their data collection practices were not unlawful at that time.

[19] *See, e.g.*, Cecilia Kang, *Preteens' Use of Instagram Creates Privacy Issue, Child Advocates Say*, WASH. POST, May 15, 2013, *available at*: http://articles.washingtonpost.com/2013-05-15/business/39274733_1_instagram-privacy-advocates-child-advocates.

[20] *See, e.g.*, Perri Klass, M.D., *How Advertising Targets Our Children*, N.Y. TIMES, Feb. 11, 2013, *available at*: http://well.blogs.nytimes.com/2013/02/11/how-advertising-targets-our-children/.

[21] TEENS, SOCIAL MEDIA, AND PRIVACY, *supra* n.12 at 3.

Information collected about children has included full names, screen names, phone numbers, email addresses, street addresses, specific geolocation data, photographs, and videos. "A [June 2013] *Wall Street Journal* examination of forty popular and free child-friendly apps on Google's Android and Apple, Inc.'s iOS mobile operating systems found that nearly half transmitted to other companies a device ID number, a primary tool for tracking users from app to app."[22] Seventy percent of these apps also "passed along information about how the app was used, in some cases including the buttons clicked and in what order."[23]

It is important to note, however, that, in its latest review of COPPA, the FTC analyzed websites' and apps' collection of information used to support internal operations and explicitly permitted such use in the latest COPPA rule revisions.[24] As one Workgroup member pointed out, this information helps app developers eliminate bugs and improve the user experience. Collected analytics information helps developers tailor apps for special-needs children and support language and mathematics development.

Privacy Disclosures for Child-Oriented Websites and Apps are Often Confusing or Nonexistent

Unfortunately, many child-oriented websites and apps lack clear privacy disclosures for the information they collect, and many provide no disclosures at all. A 2012 FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, examined 400 apps directed at kids and found that "most apps failed to provide *any* information about the data collected through the app, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data."[25] That report also found "a high incidence of interactive features within the apps that, in most cases, were not disclosed to users," such as in-app advertising, which was present in 58% of the apps reviewed but disclosed prior to download only 15% of the time.[26] The Report further observed that this "transmission of kids' information to third parties that are invisible and unknown to parents raises concerns about privacy, particularly because the survey results show that a large number of apps are transmitting information to a relatively small number of third parties."[27]

Where privacy disclosures are provided, they are often presented in dense legalese that is confusing to parents. For example, the Workgroup members were shown the privacy policy of Nickelodeon, which has a website that is clearly directed at children (although not necessarily only children under 13). The company discloses that its website collects registration information and information about third-party social networks and automatically collects device

[22] Jeremy Singer-Vine & Anton Troianovski, *How Kid Apps Are Data Magnets*, WALL ST. J., June 27, 2013, *available at* http://online.wsj.com/article/SB10001424127887324520904578553662943430052.html.
[23] *Id.*
[24] *See* 16 C.F.R. § 312.2 (defining "Support for the internal operations of the Web site or online service"); *see also id.* §§ 312.5(c)(7) & 312.12(b).
[25] FED. TRADE COMM'N, STAFF REPORT, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 4 (Dec. 2012); *see also* FED. TRADE COMM'N, STAFF REPORT, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DIS*APP*OINTING 13 (Feb. 2012).
[26] *Id* at 6.
[27] *Id.* at 15.

information.[28] Nickelodeon also uses at least 20 different third-parties in conjunction with its website, each of which may collect, use, and disclose information collected from website visitors. The privacy implications of this web of collection and sharing for children's data are often difficult for parents to tease out.

Workgroup members noted that compliance with the updated COPPA Rule should ensure clearer, more prominent privacy disclosures.[29] They also noted that the U.S. National Telecommunications and Information Administration (NTIA) has recently introduced a short form notice code of conduct to promote transparency in mobile app practices that was the result of an intensive multistakeholder process among consumer and industry advocates.[30] Adherence to this code of conduct should improve privacy disclosures as well.

Issue 2: Current and Forthcoming Federal and State Regulation of Children's Online Privacy and Online Advertising and Associated Data Collection

Federal: COPPA and the updated COPPA Rule

As discussed in the introduction, the Children's Online Privacy Protection Act ("COPPA" or "Act"), enacted in 1998, is the main federal statute governing the protection of personal information collected from "children online," a term that COPPA defines as individuals under the age of 13. *See* Appendix B. COPPA makes it "unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child" without first providing notice and obtaining verifiable parental consent.[31] COPPA empowers the FTC to adopt regulations (now known as the "COPPA Rule") regarding the requirements for providing notice and obtaining verifiable parental consent, among other matters covered by the Act.[32] *See* Appendix C. It also authorizes the FTC and state attorneys general to enforce violations of the Act and the accompanying regulations,[33] and treats any violation of the Act as an unfair and deceptive trade practice prohibited by the Federal Trade Commission Act.[34] To encourage compliance with the COPPA Rule, COPPA provides safe harbors for operators that

[28] The registration information includes (a) birth date; (b) gender; (c) country; (d) state; (e) zip code; (f) user name and password; (g) wireless telephone number; (h) email address; and (i) other profile information such as avatar preferences, communications preferences, and interests. The device information includes (j) IP address for desktop and laptop computers; (k) unique device identifier ("UDID") for mobile devices; (l) information about the websites visited before and after visiting the website; (m) information about the web pages and advertisements viewed – and links clicked – within the Nickelodeon website; and (n) information collected through the use of unique identifiers such as cookies. *See* http://www.nick.com/info/privacy-policy.html#I.

[29] *See* 16 C.F.R. § 312.4(d).

[30] The full code of conduct is available here: http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf. For more information, including statements by participants in the multistakeholder process, see here: http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[31] 15 U.S.C. § 6502(a).

[32] 15 U.S.C. § 6502(b).

[33] 15 U.S.C. §§ 6502(c) and 6504.

[34] 15 U.S.C. § 6502(c).

"follow[] a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, [and] approved" by the FTC.[35]

COPPA defines protected "personal information" to mean "individually identifiable information about an individual collected online," including the following:

> (A) a first and last name;
> (B) a home or other physical address including street name and name of a city or town;
> (C) an e-mail address;
> (D) a telephone number;
> (E) a Social Security number;
> (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
> (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described [above].[36]

The original COPPA Rule, which went into effect in April 2000, contained its own definition of "personal information" and put in place limits on collection of personal information from children. With rapid changes in technology – including changes in the way children use and access the Internet, such as the increased use of mobile devices and social networking, what information can be collected about individuals online, and the ways in which that information can be collected – the FTC undertook a process to review and revise the Rule, beginning in 2010.[37] This process included multiple public comment periods.[38]

---

[35] 15 U.S.C. § 6503(a).

[36] 15 U.S.C. § 6501(8). For the sake of comparison, Maryland's Personal Information Protection Act defines protected "personal information" to mean the following:

> an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:
>
> (i) A Social Security number;
> (ii) A driver's license number;
> (iii) A financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or
> (iv) An Individual Taxpayer Identification Number.

Md. Code Ann., COM. LAW § 14-3501(d). *See id.* STATE GOV'T § 10-1301(c); *see also id.* CORR. SERVS. § 3-511(c) (defining "personal information" to mean an individual's Social Security number or credit card or financial information); CTS. & JUD. PROC. § 1-205(a) (Social Security or driver's license number); REAL PROP. § 3-111(a) (same); STATE GOV'T §§ 2-1804(a) & 8-504(a) (same); STATE GOV'T § 10-611(g) (defining "personal information" to mean "information that identifies an individual including an individual's address, driver's license number or any other identification number, medical or disability information, name, photograph or computer generated image, Social Security number, or telephone number"); STATE GOV'T § 10-618(m) (defining "personal information" to mean "an address; a phone number; an electronic mail address; or directory information").

[37] *See* http://business.ftc.gov/content/coppa-rulemaking-and-rule-reviews.

The FTC's amended COPPA Rule, adopted in December 2012 and effective July 1, 2013, seeks to strengthen the existing COPPA Rule's limits on the extent to which information can be collected about children without parental notification and consent.[39] The Rule expands the definition of "personal information" as it pertains to children to include "persistent identifiers" that can recognize users over time and across different websites or online services (e.g., cookies, device IDs, and IP addresses), geolocation information, screen names and user names where they function in the same manner as online contact information, and photos, videos and audio files containing a child's image or voice. In this way, it makes more forms of third-party data collection unlawful in the absence of parental notice and consent. It also updates and expands the ways in which websites and apps can obtain verifiable parental consent. Lastly, it strengthens the existing Rule's confidentiality, security, and integrity provision by adding a requirement that operators take reasonable steps to release children's personal information only to parties capable of maintaining its security.

Federal: "Do Not Track Kids" Act

On November 14, 2013, Senator Edward J. Markey (D-Mass.) and Representative Joe Barton (R-Texas), along with Senator Mark Kirk (R-Ill.) and Representative Bobby Rush (D-Ill.), introduced legislation to expand upon the protections offered by COPPA and the COPPA Rule. The "Do Not Track Kids" Act of 2013 (S. 1700 and H.R. 3481) amends COPPA and includes new protections for teens ages 13-15 – a group that is highly connected to the Internet and potentially vulnerable to misuse of personal information shared online. The Act also establishes a requirement for a "Digital Marketing Bill of Rights for Teens" that limits the collection of personal information of teens, including geolocation information of children and young teens; creates an "Eraser Button" for parents and children by requiring companies to permit users to eliminate publicly available personal information content about children and young teens posted by the user (when technologically feasible); prohibits Internet companies from collecting personal and location information from children under 13 without parental consent and teens 13 to 15 years old without the teen's consent; requires companies to obtain the consent of parents of children under 13 and the consent of teens aged 13 to 15 before sending targeted advertising to such children and teens; and requires online companies to explain the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information. *See* Appendix D.

The bill has received the endorsement of the American Academy of Child and Adolescent Psychiatry, American Academy of Pediatrics, American Family Association, Campaign for a Commercial-Free Childhood, Center for Digital Democracy, Center for Science in the Public Interest, Childhelp, Children Now, Common Sense Media, Communication Workers of America, Consumer Federation of America, Consumer Watchdog, Consumers Union, Conversation Media, Identity Theft 911, Islamic Society of North America, Massachusetts Medical Society, National Collaboration for Youth, Parent Teacher Association,

[38] *See id.*
[39] *See* 78 Fed. Reg. 3972 (2013), *available at*: http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf (FTC's order revising the COPPA Rule).

Safe Communications, Inc., United Church of Christ, U.S. Conference of Catholic Bishops, Virtual World Computing, and Voices of America's Children. The bill has also been criticized by children's advocates such as NetFamilyNews.[40]

California: Online Privacy Protection Act

California was the first state in the country to pass its own distinct online privacy law, the California Online Privacy Protection Act, known as "CalOPPA." CalOPPA, which went into effect in 2004, requires an operator of a commercial website or online services that collects "personally identifiable information" ("PII") through the Internet about California consumers who use or visit that website or online service to "conspicuously post its privacy policy." The privacy policy must: (1) identify the categories of PII that the operator collects through its website or online service about individual consumers who use or visit it; (2) identify the categories of third-party persons or entities with whom the operator may share that PII; (3) if it offers a process for review and editing of PII by the consumer, provide a description of that process; (4) describe the process by which it notifies consumers who use or visit its website or online service of material changes to its privacy policy for that website or online service; and (5) contain the privacy policy's effective date. *See* Appendix E.

CalOPPA defines PII, "conspicuously post," and other key terms in detail, and defines "consumer" to mean "any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." Accordingly, CalOPPA's protections apply to California consumers of all ages, including children. Websites that collect information from children residing in California must abide by the provisions of CalOPPA, separate and apart from their obligations under COPPA.

California: "Shine the Light" Law

The same year California passed CalOPPA, it also passed another privacy law that has become known as the "Shine the Light" law.[41] The "Shine the Light" law, which went into effect in 2005, requires those companies that do business with California customers and wish to share the customers' "personal information" with third parties for direct marketing purposes to (1) obtain opt-in consent from those customers to share their personal information with those third parties, (2) allow those customers to opt out of information sharing with those third parties, or (3) disclose, in detail, how they are sharing customers' personal information with third parties (including providing the names and addresses of all of those third parties).[42]

The law defines "customers" broadly; California children and teens can be considered "customers" entitled to the law's protections over personal information. The law also defines "personal information" broadly, encompassing any information that, when disclosed to a third

[40] Ann Collier, *Flawed Early Laws of Our New Media Environment*, NetFamilyNews.org, 2013, *available at*: http://www.netfamilynews.org/flawed-early-laws-of-our-new-media-environment.
[41] CAL. CIV. CODE § 1798.83.
[42] Utah has a similar third-party notification requirement. UTAH CODE ANN. § 13-37-201(3)(a).

party, identifies, describes, or is able to be associated with an individual, including not just name and address and email address but also identifiers like race, religion, occupation, education, political party affiliation, and medical condition. The law's definition of "personal information" specifically includes children's ages, genders, email addresses and physical addresses.

The law defines "business" more narrowly. To be covered by the law, a business must have at least 20 employees (whether full-time or part-time), an established business relationship with a California customer, and a history of either having disclosed personal information to third parties for direct marketing purposes or having known or had reason to know that third parties were using the personal information it shared for direct marketing purposes. The law does not apply to federal financial institutions.[43]

California: "Eraser Button" Law

California recently enacted *Privacy Rights for California Minors*, SB 568, which Governor Jerry Brown signed into law on September 23, 2013. The law – known as the "eraser button" law – received bipartisan support and was created with input from Facebook and Google. It will take effect on January 1, 2015, and is aimed at extending and supplementing the new COPPA Rule. *See* Appendix E. The law is designed to increase privacy protections for children and adolescents on the Internet by allowing them to remove their postings on internet and social media sites, and by prohibiting the advertising of harmful products that are illegal for them to use (like alcohol, tobacco and guns), on websites specifically targeted to minors.

The new law prohibits operators of websites, online services, and online or mobile apps from knowingly marketing certain products to "minors," a term defined as anyone under the age of 18. The law thus has a broader reach than COPPA, which applies only to under-13s. Further, the law extends to operators *and* to advertising services that are notified that the site, service, or app is directed to minors. The forbidden products identified by the law are clearly listed and are products that are already prohibited from being sold to minors by other existing California statutes.

In addition, the law includes a removal or right-to-erase provision that requires websites, services, and apps to erase content posted by minor registered users upon their request. However, companies are still allowed to store the removed information on their server if it is rendered invisible to other users or the public, and are not required to "erase" content that was posted or republished by third parties.

Some have criticized the California bill for requiring companies to be *more* intrusive, in that they would need to collect more information about users – e.g., about their age and whether they reside in California – in order to ensure compliance. Others say that this criticism is misplaced, because the law does *not* require companies to collect more information about their users than they already do. The law applies to websites, online services and apps that are

[43] The full text of the law is available here: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

directed to minors under 18 or that have "actual knowledge" that a user is under 18 (e.g., through "age gating" or user registrations). The law specifically provides that it shall not be construed to require operators "to collect age information about users."[44] A concern has also been raised that most Internet companies span multiple states and so could find it difficult to comply with various state laws if other states enact conflicting laws.

California: "Do Not Track" Law

California also recently enacted AB 370, which Governor Brown signed into law on September 27, 2013. This law – known as the "Do Not Track" law – amends CalOPPA, and, like CalOPPA, applies to children and adults. Under the "Do Not Track" law, an operator of a commercial website or online service that collects personally identifiable information through the Internet about California consumers who use or visit that website or online service must disclose to consumers how it responds to "do not track" signals or other mechanisms that provide consumers a choice regarding the collection of PII about an individual consumer's online activities over time and across different websites or online services. The law also requires the operator to disclose whether third parties may collect PII when a consumer uses that operator's website or service. *See* Appendix E.

It should be noted that this law does *not* require an operator to honor a consumer's "do not track" request or signal; it simply requires the operator to disclose how it will respond to that request. The law also does not define what "do not track" means, nor does it define what "'do not track' signals or other mechanisms" means. Some have argued that this law does not improve consumers' protections against being tracked online. Others say that it better informs consumers about which websites and online services track them, enabling them to vote with their feet by using different services if they wish not to be tracked online.

Illinois: Age Verification for Social Networks (*Proposed*)

In 2008, Illinois legislators introduced a bill, entitled the "Social Networking Website Access Restriction Act" (H.B. 4874), that would have required owners of social network websites to implement procedures for verification of the age and information of anyone having a webpage and obtain and maintain in a database the written permission of the parent or guardian of each minor who is allowed to access that website. The bill further would have required the owners of these websites to give each parent or guardian "unrestricted access" to the social network profile of the minor under his or her supervision.[45]

The law was not enacted, partially due to concerns over the free speech rights of minors. As was pointed out to the Workgroup members, while children and young teens might not have unlimited rights to free speech, placing limitations on the speech rights of older teens raises challenging questions. As the Supreme Court has written, "It is well settled that a State or

[44] Section 22581(e).
[45] The full text of the bill is available here: http://www.ilga.gov/legislation/95/HB/PDF/09500HB4874lv.pdf.

municipality can adopt more stringent controls on communicative materials available to youths than on those available to adults. Nevertheless, minors are entitled to a significant measure of First Amendment protection." *Erznoznik v. Jacksonville*, 422 U.S. 205, 212 (1975) (internal citation omitted); *see Brown v. Entm't Merchs. Ass'n*, 131 S. Ct. 2729, 2735-2736 (2011).

Maine: Predatory Marketing to Minors (*Repealed*)

In 2009, Maine passed a children's online privacy bill entitled "An Act to Prevent Predatory Marketing Practices against Minors" (L.D. 1677). The Act prohibited the disclosure and use of personal information collected from a minor and restricted the collection of that information from a minor for marketing purposes without verifiable parental consent.[46] The law allowed for both state attorney general enforcement – under the state consumer protection act – and private enforcement actions for violations, with the ability to obtain attorney's fees and treble damages if the violations were willful.

The law was subsequently challenged in a lawsuit filed by NetChoice, which claimed that it was overbroad in ways that violated the First Amendment, was prohibited by the Dormant Commerce Clause, and was preempted by COPPA. Maine's Attorney General reviewed the law and found constitutional infirmities, and so agreed not to enforce it. As a result, the lawsuit was dismissed, and the law was later repealed. Workgroup members learned that one of the reasons the law drew strong opposition was that it had the unintended consequence of preventing colleges from being able to advertise to high school students.

Massachusetts & New York: "K12 Student Privacy & Cloud Computing Act" (*Proposed*)

Both Massachusetts and New York have proposed legislation to prohibit Internet service providers who offer "cloud" computing services to K-12 educational institutions from processing student data for commercial purposes. *See* Appendix E. Cloud computing services enable individuals and institutions to store data on remote servers rather than on their own servers and equipment, freeing up storage space and often lowering overhead costs. It also allows for innovative forms of web-based student collaboration. Maryland schools have already begun to use cloud computing services. In 2010, the Maryland Education Enterprise Consortium (MEEC) and the University of Maryland, Baltimore County (UMBC) announced an agreement to make Google's "Apps for Education" suite, which includes apps with cloud storage components like Google Drive and Google Docs, available to the 189 K-12 and higher educational institutions in its membership.[47]

[46] The full text of the law is available here: http://www.mainelegislature.org/legis/bills/bills_124th/chappdfs/PUBLIC230.pdf.

[47] *Maryland Education Enterprise Consortium and UMBC Announce Agreement with Google*, UMBC NEWS, Aug. 6, 2010, *available at*: http://www.umbc.edu/blogs/umbcnews/2010/08/maryland_education_enterprise.html.

However, the location of student data on private servers raises questions about its potential further uses and misuses.[48] For example, cloud computing services may resell that data for commercial purposes, as has been reported in some jurisdictions.[49] Accordingly, legislators are seeking to ensure that cloud service providers for educational institutions in their state do not use the student data they collect for purposes that could threaten students' privacy or commercially exploit the providers' unique access to students' personal information.[50] Both the Massachusetts and New York bills are still under consideration. *See* Proposed Recommendation 1 below. Additionally, a group of parents in New York have filed suit to block the school system from transferring student data to a cloud computing service, expressing concern about the security of students' information.[51]

Michigan & Utah: "No Spam" Law

In 2004, following in the footsteps of the federal government's passage of the CAN-SPAM Act, which established standards for sending commercial emails and preventing "spam" emails, Michigan and Utah passed legislation that created "no spam" protections for children's email addresses.[52] Both laws are aimed at reducing unwanted advertising to children. The stated intent of the Michigan law, for example, is "to provide safeguards to prevent certain messages regarding tobacco, alcohol, pornography, gambling, illegal drugs, and other illegal products from reaching the minor children of this state."[53]

One major concern about these state laws is that they each call for the registry to be established and operated by a private third-party company.[54] The company selected by both states to perform this function was Unspam Technologies, Inc.[55] State reliance on Unspam concerns some privacy advocates because it puts those states in the position of having to put in private hands an extensive list of children's email addresses, which presents a data security risk. There is also a view that these laws mainly served to advance the economic interests of Unspam.

---

[48] *See, e.g.*, Bradley Shear, *Maryland Schools Weak on Digital Privacy*, BALT. SUN, Oct. 11, 2012, *available at*: http://articles.baltimoresun.com/2012-10-11/news/bs-ed-digital-privacy-20121011_1_google-apps-maryland-schools-privacy-laws.

[49] *See Experts, Parents, Lawmakers Blast Database Providing Personal Student Information To Vendors*, CBS New York, March 14, 2013, *available at*: http://newyork.cbslocal.com/2013/03/14/experts-parents-lawmakers-blast-database-providing-personal-student-information-to-vendors/.

[50] It should be noted that, to the extent K-12 cloud computing service providers collect "education records" as defined in the Family Educational Rights and Privacy Act ("FERPA"), they and the schools contracting with them have FERPA obligations to protect student data.

[51] Chau Lam, *Parents' suit aims to stop state's education cloud data plan*, NEWSDAY, Nov. 13, 2013, *available at*: http://www.newsday.com/long-island/education/parents-suit-aims-to-stop-state-s-education-cloud-data-plan-1.6432109.

[52] "Michigan Children's Protection Registry Act," MICH. COMP. LAWS §§ 752.1061—.1068 (2004); "Utah Child Protection Registry Act," UTAH CODE §§ 13-39-101—304 (2004).

[53] MICH. COMP. LAWS § 752.1061(2).

[54] MICH. COMP. LAWS 752.1063(1).

[55] *See* http://www.unspam.com/services.html?section=comp_list&vid=1hsfjhe0srpbgv312r4j06tno6; *see also* http://www.unspam.com/projects.html?project=michigan_childrens_protection_registry&vid=89b476ia38dop3aflnchd4fbd6 (Michigan registry); http://www.unspam.com/projects.html?project=donotcontact_utah_gov (Utah registry).

Nebraska and Pennsylvania: False Statements on Privacy Policies

Nebraska and Pennsylvania both have longstanding provisions in their state consumer protection statutes that make it a deceptive trade practice to make a false or misleading statement in a privacy policy that is published on the Internet. These provisions are specific to false or misleading statements in privacy policies "regarding the use of personal information submitted by members of the public."[56] Both statutes are understood to apply to children and adults, as they are not audience-specific but rather conduct-specific and do not define "members of the public." Note, however, that Maryland's Attorney General has successfully brought actions under Maryland's Consumer Protection Act against Internet companies that misrepresented their privacy policies. *See, e.g.*, *In re Toysmart.com, In re eToys.com* and *In re Egghead.com.*

<u>Issue 3</u>: The Effects on Children of Online Behavioral Advertising, Native Advertising, Social Advertising, and Other Forms of Online Advertising

Online Advertising and Children's Perceptions

The Workgroup learned that, due to children's early developmental state, advertising to children – both online and off – is highly problematic. Children under 8 years of age lack the cognitive ability to critically process advertising.[57] Children ages 10 to 12 still require cues to critically process advertising and have inadequate media literacy skills. And even children 13 and over are not fully developed and are prone to impulsivity, and vulnerable to peer pressure and emotional appeals. These cognitive vulnerabilities may become more pronounced when children are targeted with one-to-one advertising, the tailored, targeted model of advertising that is made possible by Internet technology.

As early as 1995, children were being targeted for commercial purposes on the Internet without their knowledge. A website called KidsCom, which was directed at kids ages 4 to 15, drew kids in with educational games and chat ability and was even praised for its educational content. However, it was later revealed that the website was essentially an online market-research tool, "designed to elicit a wealth of demographic, behavioral, and preference information from children."[58] The website asked for personal information from children through the registration process and various questionnaires and then rewarded them with prizes for

[56] NEB. REV. STAT. § 87-302(a)(14) ("A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, he or she . . . [k]nowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."); 18 PA. CONS. STAT. § 4107(a)(10) ("A person commits an offense if, in the course of business, the person . . . knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.").

[57] *See supra* n.15. *See also* D. Kunkel & J. Castonguay, *Children and Advertising: Content, Comprehension, and Consequences*, *in* D. SINGER AND J. SINGER (EDS.), HANDBOOK OF CHILDREN AND THE MEDIA 395-41 (2012); D. R. John, *Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research*, 26 J. CONSUMER RESEARCH 183, 183-213 (1999).

[58] KATHRYN MONTGOMERY, CENTER FOR MEDIA EDUCATION, WEB OF DECEPTION: THREATS TO CHILDREN FROM ONLINE MARKETING 67 (1996).

sharing that information.[59] While adults would perhaps have been able to pick up on the marketing elements of the website, children were not disposed to notice that function.

The spread of Internet use and advancement of Internet technology has led to more sophisticated marketing efforts that pose challenges for children, given their cognitive limitations.[60] Four primary online marketing trends were identified for the Workgroup. The first is the continued integration and blurring of advertising and content. For adults, this integration appears most commonly in "native advertising," advertising content that appears on a website alongside that website's main content in ways that look like the main content (e.g., on a news website, an article advertising a new product appearing alongside other news articles).[61] For children, this integration is most commonly seen in "Advergames," mentioned above, which are built to promote the purchase of a product but appear to be built as simply a fun activity.[62] Research has shown that playing these games induces a "flow state," where the mind is not consciously engaged and capable of critically evaluating a commercial message.[63] These games also blur the lines between real money and fake money; in many of them a child can "purchase" items using what may appear to be gems or other fake items, but these so-called "in-app" purchases may be tied to real credit cards.[64] Another example is interactive ad experiences known as "immersion" experiences, which are not presented as ads but which nonetheless constitute advertising. The Workgroup was shown, as an illustrative example, "Asylum 626," an immersion experience that appeared to be a horror-themed online game but that was actually designed to promote two flavors of Doritos.[65] Without labels of some kind identifying these advergames and immersion experiences as advertising, children are unable to detect their advertising purposes.[66]

---

[59] *Id.* at 68.

[60] *See, e.g.*, Sandra L. Calvert, *Children as Consumers: Advertising and Marketing*, 18 FUTURE OF CHILDREN 205 (2008) ("All these marketing strategies, says Calvert, make children younger than eight especially vulnerable because they lack the cognitive skills to understand the persuasive intent of television and online advertisements.").

[61] *See, e.g.*, Edward Wasserman, *Advertising Goes Native, and Deception Runs Free*, HUFFINGTON POST, Jan. 30, 2013, *available at*: http://www.huffingtonpost.com/edward-wasserman/native-advertising-atlantic-scientology_b_2575945.html.

[62] *See, e.g.*, Lorraine J. Weatherspoon et al., *Consistency of Nutrition Recommendations for Foods Marketed to Children in the United States, 2009-2010*, 10 PREVENTING CHRONIC DISEASE 130099 (2013) (identifying 143 websites that marketed foods to children aged 2 through 11 years through advergames).

[63] Dongseong Choi & Jinwoo Kim, *Why People Continue to Play Online Games: In Search of Critical Design Factors to Increase Customer Loyalty to Online Contents*, 7 CYBERPSYCHOLOGY & BEHAVIOR 1 12-13 (2004).

[64] Hilary Osborne, *OFT Warns Free Online Games Pressure Children into In-App Purchases*, THE GUARDIAN, Sept. 25, 2013, *available at*: http://www.theguardian.com/money/2013/sep/26/free-online-games-children-apps (reporting on an investigation by the U.K. Office of Fair Trading that found that some online games included "potentially unfair and aggressive commercial practices" and that "children's inexperience, vulnerability and credulity" were being exploited).

[65] *Doritos Celebrates Halloween by Bringing Back Two Flavors from the Past and Launching Asylum* 626, SNACK CHAT, Oct. 1, 2009, *available at*: http://www.snacks.com/good_fun_fritolay/2009/10/doritos-celebrates-halloween-by-bringing-two-flavors-back-from-the-past-and-launching-asylum-626.html.

[66] It is the understanding of Workgroup member Family Online Safety Institute that advergames tend not to be marketed to children, and Workgroup member Direct Marketing Association noted that Asylum 626, in particular, is an age-gated advergame, requiring all users to be 18 or older to participate. However, the FTC has noted that advergames are often marketed to children, for example describing one case where "children were directed to hold a cereal box up to a webcam in order to interact with an advergame." FED. TRADE COMM'N, A REVIEW OF FOOD MARKETING TO CHILDREN AND ADOLESCENTS: FOLLOW-UP REPORT 70 (Dec. 2012), *available at*: http://www.ftc.gov/reports/review-food-marketing-children-adolescents-follow-report.

The second trend is the use of "fan" pages and other social media pages that encourage interaction with the page as a way of engaging children and youth and, in the process, creating brand awareness and fostering brand loyalty. Children are drawn to the Internet as a means of self-expression and identity exploration, and these pages allow them to express themselves while also developing a positive association with a brand.[67] The children may not be aware of that underlying advertising purpose when they interact with the site, and that is part of what makes the technique successful. Of course, many social media pages with "fan" pages for brands, like Facebook, are not open to children, reducing their exposure.[68]

The third trend is the integration of data collection with the user experience. As with KidsCom, many apps geared at children have included, as part of creating an account, the collection of lots of information, including specific location information, and many of these apps have also encouraged children to submit still more of their information, like their photographs. A recent McDonald's Happy Meal viral advertising campaign encouraged children to submit photos of themselves to email to friends, for example. That campaign had to be reconfigured after it was discovered that these photos could be easily accessible by members of the public, greatly threatening children's privacy.[69] Children are not able to see how collecting large quantities of information about them can lead to the creation of marketing profiles.

The fourth trend is the rapid adoption of mobile devices by children,[70] a trend that has created expanded opportunities for companies to collect geolocation information.[71] Children

---

[67] Margie K. Shields & Richard E. Behrman, *Children and Computer Technology: Analysis and Recommendations*, 10 CHILDREN & COMPUTER TECHNOLOGY 12 (2000).

[68] It should be noted that, despite Facebook's policy that users be at least 13, many children nonetheless are on Facebook. A 2012 survey by Consumer Reports found that more than 5.6 million children under 13 had Facebook accounts. *See, e.g.*, *Consumer, Privacy, Health, Child Groups: Facebook Space for Preteens Must Protect Privacy, Be Ad-Free and Marketing-Free* ConsumersUnion, June 18, 2012, *available at*: http://consumersunion.org/news/consumer-privacy-health-child-groups-facebook-space-for-preteens-must-protect-privacy-be-ad-free-and-marketing-free/. Facebook has been working to address this issue.

[69] Katy Bachman, *McDonald's Backs Off Online Viral Marketing to Kids, Changes Follow Complaint Filed with FTC*, ADWEEK, Oct. 23, 2012, *available at*: http://www.adweek.com/news/technology/mcdonalds-backs-online-viral-marketing-kids-144716; *see* Press Release, Maryland Office of the Attorney General, *Attorney General Gansler Recognizes Changes to McDonald's Child-directed Website*, Oct. 25, 2012, *available at*: http://www.oag.state.md.us/Press/2012/102512a.html.

[70] As mentioned above, *supra* p. 2, recent research has shown that almost twice as many children are using mobile media now as there were just two years ago, and the average amount of time children spend using mobile devices has tripled. *See also* Anton Troianovski, *Feathers Fly as New Rules Loom for Kids' Apps*, WALL ST. J., April 4, 2013, *available at*: http://online.wsj.com/news/articles/SB10001424127887323916304578403003629353068 (reporting that 37% of children ages 4-5, 35% of children ages 6-8, 38% of children ages 9-11, and 47% of children ages 12-14 use smartphones, iPod Touches, and tablets).

[71] The collection of some types of geolocation information from children has always been considered to violate COPPA. As initially adopted, the COPPA Rule's definition of "personal information" included a "home or other physical address including street name and name of a city or town." 16 C.F.R. § 312.2. In its 2011 Notice proposing revisions to the COPPA Rule, the FTC explained that "any geolocation information that provides precise enough information to identify the name of a street and city or town is covered already under existing paragraph (b) of the definition of 'personal information.'" Children's Online Privacy Protection Rule, Proposed Rule, 76 Fed. Reg. 59804, 59813 (Sept. 27, 2011). In updating the COPPA Rule, the FTC added to the definition of "personal information" "Geolocation information sufficient to identify street name and name of a city or town." The Statement of Basis and Purpose explains that "because geolocation information can be presented in a variety of formats (e.g., coordinates or a map), and in some instances can be more precise than street name and name of city or

may not even be aware that their location information is being collected when they use mobile devices.[72]

Workgroup members agreed that the online space is changing rapidly, and more research needs to be done to explore the effects of online advertising on children's perceptions.

Online Advertising and Children's Health

The Workgroup also learned that exposure to online advertising shapes children's consumption habits. For example, studies have shown strong associations between increases in advertising for non-nutritious foods and rates of childhood obesity.[73] A report by the Kaiser Family Foundation found that 85% of the top food brands had a corporate or brand website that would likely appeal to children.[74] Studies have documented both that a high percentage of advertisements targeting children feature unhealthy products associated with weight gain and that exposure to these advertisements increases consumption of these products.[75]

Research has also shown a substantial relationship between children's exposure to tobacco and alcohol ads and positive attitudes toward consumption of such products.[76] With the spread of social media and ad-supporting gaming popular among children, many such companies promoting brand awareness have new channels to expose children to their products and build brand loyalty early.[77] This increased exposure has impacts on children's health in the future.

Issue 4: Best Practices Used by the Internet Industry and the Mobile Application Industry to Protect Children's Online Privacy

Self-Regulatory Standards

Some members of the Internet industry and mobile application industry have developed sets of self-regulatory standards that offer best practices for the treatment of personal information collected online, including from children. The Direct Marketing Association (DMA), Direct

---

town, the Commission proposed making geolocation information a stand-alone category within the definition of personal information." 78 Fed. Reg. at 3982. The effect of this change is that "covered operators will be required to notify parents and obtain their consent prior to collecting geolocation information from children." *Id.* at 3983.

[72] *See, e.g.*, Lorraine McCarthy, *Mobile App Developer Settles New Jersey Claims Over Collection of Children's Data*, Bloomberg BNA, Dec. 2, 2013, *available at*: http://www.bna.com/mobile-app-developer-n17179880410/ (describing a settlement with a company that collected geolocation information from children through a geolocation scavenger hunt featuring cartoon characters).

[73] *See generally* FED. TRADE COMM'N, A REVIEW OF FOOD MARKETING TO CHILDREN AND ADOLESCENTS: FOLLOW-UP REPORT (Dec. 2012).

[74] ELIZABETH S. MOORE, IT'S CHILD'S PLAY: ADVERGAMING AND THE ONLINE MARKETING OF FOOD TO CHILDREN, KAISER FAMILY FOUNDATION 27 (2006).

[75] *See, e.g.*, BRIAN L. WILCOX ET AL., AMERICAN PSYCHOL. ASS'N, REPORT OF THE APA TASK FORCE ON ADVERTISING AND CHILDREN 6 (2004) .

[76] *Id.*

[77] *See, e.g.*, Josh Wolford, *E-Cigarette Ad Pops Up Inside Kids iPad Game*, WEBPRONEWS, Oct. 25, 2013, *available at*: http://www.webpronews.com/e-cigarette-ad-pops-up-inside-kids-ipad-game-2013-10.

Advertising Alliance (DAA), Interactive Advertising Bureau (IAB), and Network Advertising Initiative (NAI) all have such self-regulatory standards in place.

The DMA, for example, has "Guidelines for Ethical Business Practices" that include four provisions relating to marketing to children and collecting information about children. They are excerpted below:

> **Article #13: Marketing to Children**
> Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online, via wireless devices such as a mobile phone or in any other medium, marketers should predetermine whether the use of the child's data for marketing purposes or the sending of marketing material to the child is permitted under federal law, such as the Children's Online Privacy Protection Act (COPPA), or state law. Where marketing to children is permitted by law, marketers should ensure the marketing is suitable for the child, taking into account the age range, knowledge, sophistication, and maturity of their intended audience.
>
> **Article #14: Parental Responsibility and Choice**
> Marketers should provide notice and an opportunity to opt out of the marketing process so that parents have the ability to limit the collection, use, and disclosure of their children's names, addresses, or other personally identifiable information.
>
> **Article #15: Information From or About Children**
> Marketers should take into account the age range, knowledge, sophistication, and maturity of children when collecting information from them. Marketers should limit the collection, use, and dissemination of information collected from or about children to information required for the promotion, sale, and delivery of goods and services, provision of customer services, conducting market research, and engaging in other appropriate marketing activities.
>
> Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected.
>
> Upon request from a parent, marketers should promptly provide the source and general nature of information maintained about a child. Marketers should implement strict security measures to ensure against unauthorized access, alteration, or dissemination of the data collected from or about children and should provide information regarding such measures upon request to the parent or guardian of the minor.
>
> **Article #16: Marketing Online to Children Under 13 Years of Age**
> Marketers should not knowingly collect personally identifiable information online or via wireless handsets or devices from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of such information, and shall provide an opportunity for the parent to prevent such use and participation in the activity.
>
> Online and wireless/mobile contact information should only be used to directly respond to an activity initiated by a child and not to recontact a child for other purposes without

prior parental consent. However, a marketer may contact and get information from a child for the purpose of obtaining parental consent.

Marketers should not knowingly collect, without prior parental consent, personally identifiable information online or via a wireless handset or device from children that would permit any offline contact with the child.

Marketers should not knowingly distribute to third parties, without prior parental consent, information collected from a child that would permit any contact with that child.

Marketers should take reasonable steps to prevent the online publication or posting of information that would allow a third party to contact a child offline unless the marketer has prior parental consent.

Marketers should not entice a child to divulge personally identifiable information by the prospect of a special game, prize, or other offer.

Marketers should not make a child's access to website or mobile content contingent on the collection of personally identifiable information. Only online contact information used to enhance the interactivity of the site is permitted.

The following assumptions underlie these online guidelines:

- When a marketer directs a site at a certain age group, it can expect that the visitors to that site are in that age range, and
- When a marketer asks the age of the child, the marketer can assume the answer to be truthful.[78]

These provisions are expected to be honored by all of the DMA's approximately 1,700 members, who account for roughly 90% of the entire online behavioral advertising space. These self-regulatory guidelines are enforced and come with penalties for non-compliance, including suspension of DMA membership[79] and expulsion from the DMA.[80] *See* Issue 6 below.

The DMA, in partnership with the IAB, NAI, and other organizations, including the Better Business Bureau, has issued a set of seven self-regulatory principles for online behavioral advertising ("OBA").[81] They are as follows: (1) The Education Principle; (2) The Transparency Principle; (3) The Consumer Control Principle; (4) The Data Security Principle; (5) The Material Changes Principle; (6) The Sensitive Data Principle; and (7) The Accountability Principle.[82]

---

[78] DIRECT MARKETING ASS'N, GUIDELINES FOR ETHICAL BUSINESS PRACTICE 11-12 (May 2011); *available at*: http://thedma.org/wp-content/uploads/DMA-Ethics-Guidelines.pdf. *See also* DIRECT MARKETING ASS'N, ONLINE BEHAVIORAL ADVERTISING (OBA) COMPLIANCE ALERT & GUIDELINES FOR INTEREST-BASED ADVERTISING, *available at*: http://www.dmaresponsibility.org/privacy/oba.shtml.

[79] *See* DIRECT MARKETING ASS'N, ANNUAL ETHICS COMPLIANCE REPORT 2012-2013 13-21 (2013), *available at*: http://form.jotformpro.com/form/32104088798966 (detailing one suspension of a DMA member for non-compliance and 12 findings of non-compliance by non-members).

[80] *See* DIRECT MARKETING ASS'N, ETHICS CASE REPORT 4 (2004), *available at*: http://www.the-dma.org/guidelines/ethicscase.pdf.

[81] DIRECT MARKETING ASS'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (July 2009), *available at*: http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf.

[82] *Id.* at 2-4.

The Sensitive Data Principle, in particular, urges member organizations to give children's data heightened protection, in accordance with COPPA. It states:

> 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.[83]

The Data Security Principle also calls for de-identification of data collected about children.[84] Ads served by DAA and DMA members include a triangle "i" logo, known as the "advertising option icon" (see at right), which indicate their adherence to these principles.[85]

The IAB's separate self-regulatory guidelines are specific to publishers, and the NAI's separate self-regulatory guidelines are specific to ad servers.

For child- and family-specific mobile apps, the Association for Competitive Technology (ACT) has two programs aimed at cultivating best practices. The first, called "ACT 4 Apps | Kids," provides app developers with education and assistance to meet privacy guidelines and build consumer trust.[86] Most members are small developers, although most of the industry leaders are also members.

"Moms with Apps" is a best practices program for members of ACT that promotes transparency for children's apps.[87] The first initiative to launch as part of this program is the "Know What's Inside" logo[88] (see at left), which signals to parents that: an app is made especially for children, the app developer makes it easy for parents to access and understand the app's privacy policy; the app explains the features of the app, so parents know what to expect; the app maker is informed about the latest privacy regulations and industry best practices and self-asserts that the app is COPPA-compliant; and that the app maker is a member of ACT. Developers sign a legally binding document about app privacy and must know the compliance of third parties that use their app. Although this initiative was just launched on July 1, 2013, there are already over 130 active members and 200 more pending. It was noted that Moms with Apps is a logo, not a seal, and does not seek to become a COPPA safe harbor.

Finally, the Children's Advertising Review Unit ("CARU") of the Council of Better Business Bureaus ("CBBB"), *see* Issue 6 below, has a "Self-Regulatory Program for Children's

---

[83] *Id.* at 16-17.
[84] *Id.* at 37.
[85] Learn more about this initiative here: http://www.aboutads.info/.
[86] http://www.act4apps.org/act-joins-forces-with-parents-app-group-to-create-act-4-apps-kids/.
[87] http://www.act4apps.org/momswithapps/.
[88] http://momswithapps.com/.

Advertising"[89] that offers a set of eight "core principles" for advertising to children,[90] as well as both general and specific guidelines for children's online privacy protection. These include the general guideline that "[a]dvertising should not be presented in a manner that blurs the distinction between advertising and program/editorial content in ways that would be misleading to children"[91] and that "[a]dvertisers who sell products and services to children online should clearly indicate to the children when they are being targeted for a sale."[92] The specific guidelines include disclosing why information is being requested in "language easily understood by a child," disclosing whether that information will be shared, sold, or distributed with/to a third party, disclosing "any passive means of collecting information from children (e.g., navigational tracking tools, browser files, etc.) and what information is being collected," and not requiring children to disclose "more personal information than is reasonably necessary to participate" in a particular online activity.[93]

Keeping Cloud Computing in K-12 Schools Non-Commercial

As mentioned above, cloud computing offers a number of benefits and opportunities to school districts, including cost savings and enhanced communication. Services that may be provided to teachers and students include email, productivity apps, learning tools and online

[89] CHILDREN'S ADVERTISING REVIEW UNIT, SELF-REGULATORY PROGRAM FOR CHILDREN'S ADVERTISING (2009), *available at*: http://www.caru.org/guidelines/guidelines.pdf.

[90] These core principles are as follows:

> 1. Advertisers have special responsibilities when advertising to children or collecting data from children online. They should take into account the limited knowledge, experience, sophistication and maturity of the audience to which the message is directed. They should recognize that younger children have a limited capacity to evaluate the credibility of information, may not understand the persuasive intent of advertising, and may not even understand that they are being subject to advertising.
> 2. Advertising should be neither deceptive nor unfair, as these terms are applied under the Federal Trade Commission Act, to the children to whom it is directed.
> 3. Advertisers should have adequate substantiation for objective advertising claims, as those claims are reasonably interpreted by the children to whom they are directed.
> 4. Advertising should not stimulate children's unreasonable expectations about product quality or performance.
> 5. Products and content inappropriate for children should not be advertised directly to them.
> 6. Advertisers should avoid social stereotyping and appeals to prejudice, and are encouraged to incorporate minority and other groups in advertisements and to present positive role models whenever possible.
> 7. Advertisers are encouraged to capitalize on the potential of advertising to serve an educational role and influence positive personal qualities and behaviors in children, e.g., being honest and respectful of others, taking safety precautions, engaging in physical activity.
> 8. Although there are many influences that affect a child's personal and social development, it remains the prime responsibility of the parents to provide guidance for children. Advertisers should contribute to this parent-child relationship in a constructive manner.

Id. at 5.

[91] *Id.* at 9.

[92] *Id.* at 11.

[93] *Id.* at 13-14.

grade books.[94] To address concerns that cloud computing service providers may collect data for advertising or other commercial purposes, different companies have created policies that offer varying degrees of protectiveness of the personal information of children and minors. Microsoft, for example, does not use any K-12 data it collects for advertising purposes; the company believes K-12 educational computing should be an ad-free environment. Universities are different animals, given the age of the student body and other factors about the university environment. There are no common industry standards at this point. Contracts for cloud computing services typically apply to an entire school system.

There are no laws directly addressing this issue or even a set of commonly accepted practices. However, Massachusetts and New York are considering legislation to govern school contracts with cloud service providers. *See* Proposed Recommendation 1 below; Appendix E. Also, Oklahoma enacted a law in May 2013, HB 1989, the Student Data Accessibility, Transparency and Accountability Act ("Student DATA Act"), which sets forth new requirements for the Oklahoma State Board of Education, including, among other things, requiring the Board to ensure that vendor contracts include an express provision that safeguards student privacy and include penalties for noncompliance.

The Center on Law and Information Policy at Fordham University School of Law has recently released a report on privacy and cloud computing in public schools that recommends that school districts using cloud services adopt contracting terms that include specification of the types of data transferred or collected, a prohibition or limitation on re-disclosure of student data, and a prohibition or limitation on the sale or marketing of student information without express parental consent, among other terms.[95]

Issue 5: Best Practices Urged by Consumer Advocates, Children's Health Advocates, and Regulators to Protect Children's Online Privacy

General Privacy Principles

The Workgroup heard about several sets of best practices urged by some consumer advocates and children's health advocates for the protection of children's privacy online. Many advocates echoed the need for "privacy by design" with child-oriented websites and apps, a concept promoted by the FTC for children's apps.[96] They also urged several other best practices that command agreement among many advocates for children's online privacy, many of which

[94] A recent study by the Center on Law and Information Policy (C.L.I.P.) at the Fordham University School of Law found that 95% of public school districts sampled "rely on cloud services for a diverse range of functions including data mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning." http://law.fordham.edu/center-on-law-and-information-policy/30198.htm; *see infra* n.95.

[95] C.L.I.P., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS (2013), *available at*: http://ir.lawnet.fordham.edu/clip/2/.

[96] FED. TRADE COMM'N, STAFF REPORT, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 4 (Dec. 2012).

are described in a 2010 Common Sense Media white paper, "Protecting Our Kids' Privacy in a Digital World."[97] These best practices are:

Do Not Track Children

Because children are inexperienced with the online marketplace and unsophisticated in their ability to navigate the privacy controls available online, the default should be for companies to not track children's locations and their activity online (consistent with COPPA's prohibitions[98]).

Do Not Allow Behavioral Advertising to Children

Children are uniquely impressionable to advertising and accordingly should not be exposed to behavioral marketing until they reach a cognitive stage that allows them to differentiate between advertising content and non-advertising content. For children under 13, this principle is already encompassed in COPPA's prohibitions.

Prohibit Online Marketing of Certain Products to Children

Regulators already control the extent to which children are exposed to advertising for products like alcohol, tobacco, and firearms. In the online environment, where it is easier than ever for a child to accidentally purchase an item – for example if his parents' billing information is tied to his mobile device – consumer advocates are urging that we do more to prevent children from being exposed to such marketing.

Make "Opt In" the Industry Standard for Children's Privacy

Because children are less sophisticated users of the Internet and mobile technologies, companies offering online products and services to children should refrain from collecting any data from them unless it is absolutely necessary to the functioning of their product or service, and even then only with explicit parental approval. Companies should also let children – under the supervision of their parents or guardians – opt in to any privacy settings that expose them to more data collection.

Make Privacy Policies Clear and Transparent

Privacy policies are generally confusing documents, and it is imperative that the privacy policies that accompany child-oriented online products and services be written in ways that are easy for parents and guardians to understand and, to the extent possible, children as well (e.g., if the app is aimed at pre-teens). Third-party ratings of the clarity and transparency of privacy policies should be encouraged to promote consumer awareness. Changes to privacy policies should be announced in ways that enable opt-in consent.

The Workgroup understood the difficulty of achieving clarity and transparency on mobile devices, where screen size limits the amount of information that can be conveyed to a consumer

[97] The full white paper is available here: http://www.commonsensemedia.org/sites/default/files/privacy_whitepaper_dec2010.pdf. To view a recent set of best privacy practices advocated in the Canadian market, see KIDS MEDIA CENTRE, AN ETHICAL FRAMEWORK FOR MARKETING AND MONETIZING DIGITAL CONTENT MEDIA FOR A 'SELF-PUBLISHED' CHILDREN'S/YOUTH AUDIENCE (July 2013), *available at*: http://kidsmediacentre.ca/downloads/Ethical-Framework-Best-Practices-kmc.pdf.

[98] *See supra* n.71 and accompanying text.

at one time. One solution to this problem that the Workgroup discussed was the use of a "Schumer box"[99] for privacy policies that highlights the most important information to consumers. This approach had already proven effective for credit card statements, which can be confusing otherwise.

Educate Parents and Children about Online Privacy

Consumers and businesses work better together if consumers are well informed about their privacy options. Efforts should be made to promote privacy literacy among children and parents, so that they can navigate in their online and mobile environments with confidence.

Apply Privacy Protections Across All Online and Mobile Platforms

As the primary entry point to the Internet continues to shift to mobile devices, companies should ensure that adequate privacy protections are in place for those devices (this applies to both the device makers and the app makers).

Other efforts to articulate privacy best practices include California Attorney General Kamala Harris's report, "Privacy on the Go: Recommendations for the Mobile Ecosystem," which offers a set of best practices for app developers, platform providers, ad networks, and others in the mobile ecosystem.[100] The report also includes particular advice related to children's privacy.[101]

European Union Privacy Principles

Principles embraced by Americans are different from those embraced in other countries. The European Union's data protection policies are much more stringent and far-reaching than those in the United States.[102] This is partly because there is a sense in European countries that you own your own data and that you have a concomitant right to remove that data from the Internet, a so-called "right to be forgotten." The right to be forgotten is not a new concept, but the proposed reforms to the European Union's Data Protection Directive are an attempt to codify it and add penalties – fines up to 500,000 euros or 1% of global profits for failure to act to help delete data. Other reforms proposed for that law are: changes in consent for minors under 13 to match COPPA (including sanctions for violators of 1 million euros or 2% of global profits); clear and simple language for users about data collection and use; rapid notification – within 24 hours – of data breaches; privacy by design; and data portability. Discussions have taken place at a very high level, and there is a push to ratify the proposals by the year's end.[103]

---

[99] See an example of a "Schumer box" here: http://i2.cdn.turner.com/money/galleries/2008/pf/0807/gallery.creditcard_offer.moneymag/images/schumer_box.jpg.

[100] CALIFORNIA DEPARTMENT OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (January 2013), *available at*: http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[101] *Id.* at 9, 14, & 16.

[102] Workgroup member Family Online Safety Institute noted that the European Union privacy principles described herein are not child-focused.

[103] To see the text of the proposed reforms – specifically the proposed new Data Protection Directive and Regulation – see here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT (Directive) and here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT (Regulation).

"Eraser Button" for Children and Teens

A compromise position between the European concept of the "right to be forgotten" and the less privacy-protective American perspective is the concept of an "eraser button" for children and teens. The idea is that children and teens, being at a stage in their cognitive development that makes them less able to conceptualize the long-term consequences of their actions, should have a greater ability to remove – or "erase" – content that they regret sharing online. Many websites and services offer a version of this already, in that they let users edit or delete content they have posted. Others, however, are less privacy-protective.

California has recently passed legislation that provides an "eraser button" mechanism for minor consumers in that state. *See* Issue 2 above; Appendix E. Some consumer advocates think that such functionality is a best practice that should be required of all child-oriented websites and online services. However, concerns have been expressed about the risks of teaching children that their content can ever be truly "erased." Education efforts focused on "think before you post" are vital. In this vein, it should be noted that the new California law expressly requires that websites and apps provide notice to minors who are registered users that removing their content "does not ensure complete or comprehensive removal of the content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user."[104]

Online Practices Consistent with Children's Health

The American Academy of Pediatrics ("AAP") offers six principles of Internet use for parents: (1) set relevant age parameters; (2) seek technical assistance and tutorials; (3) learn the fundamentals of how Internet technology works; (4) know the "roadways" of the Internet; (5) follow the rules/etiquette and make sure your kids follow the rules/etiquette; and (6) emphasize that the "real world" is offline. These principles are reflected in the educational materials that the AAP offers to parents, such as SafetyNet,[105] a website that provides parents with links and resources – from the AAP and other organizations – regarding how they can educate their children and protect their children's privacy and personal safety online.

It is very important for parents to set rules for Internet use, to enforce those rules, and to model good choices. The AAP advocates setting time limits for Internet and media use, and the AAP recommends no more than two hours of media per day for children and teens, including television, DVDs, and the Internet (also called "screen time"). For children under the age of two, the AAP recommends zero screen time.

Children's health advocates also recommend that parents and guardians put different ownership and monitoring controls in place for children, depending on their age. Children up to age 10 should not own their own devices, and parents and guardians should be actively involved in their Internet use, including through use of tools that limit their access to certain online

[104] *See infra* Appendix E, *Privacy Rights for California Minors*, Senate Bill 568, Section 22581(a)(4).
[105] http://safetynet.aap.org/.

content. Children 11-14 years of age also require adult supervision and monitoring, and they should be taught not to give out their personal information. Children 15-18 should have more freedom, but parents and guardians should be available to answer questions and to remind them what personal information should not be given over the Internet.[106]

Issue 6: The Effectiveness of Voluntary Standards as They Relate to Children's Online Privacy

CBBB's Children's Advertising Review Unit

The Children's Advertising Review Unit ("CARU") of the Council of Better Business Bureaus ("CBBB") evaluates ads for truth, accuracy, appropriateness and sensitivity to children's developing cognitive abilities. It reviews complaints and, if appropriate, will issue advice to the offending company recommending a certain course of corrective action. If CARU's recommendations are not adopted, the case may be referred to the FTC for enforcement.

COPPA was enacted to enable parents to monitor their children's online privacy. Operators must provide notice and obtain parental consent for children under 13. The law was passed in 1998, and the COPPA Rule went into effect in 2002. Since then, as noted above, the Internet has changed enormously, so the FTC has been considering amendments for a long time, and adopted amendments this year after several rounds of public comment that began in 2011.

The changes to the COPPA Rule also affected the safe harbor programs (there are five approved safe harbor entities under COPPA). CARU was the first safe harbor organization for COPPA after that law came into being. The biggest questions now are "Who must comply?" and "What does 'directed to children' mean?" Many websites and apps are offered to mixed audiences – or offered to adults but yet popular with both adults and teens, and so companies that previously thought they did not have anything to do with COPPA are contacting CARU and asking if they now fall under COPPA. Dozens of website operators have signed up to be a part of the CARU safe harbor. CARU saw a spike in applications since July 1 (when the new Rule was implemented).

CARU had to reapply to the FTC and detail its business models and technical ability in order to be deemed a safe harbor under the new FTC provisions. There is a new obligation to report annually to the FTC, starting in 2014, on the results from audits. In these reports, the names of problem cases are redacted to prevent participants in the safe harbor from being held to a different, even higher standard (since, by participating in the safe harbor, they are already demonstrating that they are being conscientious). There was no public comment on CARU's reapplication to the FTC to be a safe harbor, but it did result in a back-and-forth with the FTC.

[106] *See generally* Gwenn Schurgin O'Keeffe & Kathleen Clarke-Pearson, *The Impact of Social Media on Children, Adolescents, and Families*, 127 PEDIATRICS 4 (2011).

CARU's staff monitors thousands of commercials every year, and many do not end up being dealt with through a formal complaint process. It was noted that NAD handled 100-150 cases last year, and CARU handled 40-80. CARU prescreens between 150 and 200 commercials each year.

CARU also looks at product tie-ins, like cross-promotions with children's toys. An example along these lines was a Build-A-Bear website that included links to Pinterest and Twitter. Pinterest and Twitter are platforms that, according to their terms of service, do not accept users under 13, yet neither platform uses age gating, so under-13s frequently get accounts. This issue was referred to CARU via Common Sense Media, and, with CARU's encouragement, Build-A-Bear removed all links to Twitter and Pinterest from its site, steps not required by existing laws.

Another example of a self-regulatory review was for "Link Snacks," a brand of Beef Jerky that, in an online advertisement, asked new users for their personal information as well as other questions, such as their dream job, without regard for age. CARU noticed this ad through routine monitoring and contacted the company, and the company agreed to install a neutral age screen with a cookie to prevent users from quickly changing the birthdate they originally provided.

MPAA Advertising Administration

The Motion Picture Association of America, Inc. ("MPAA") reviews every piece of marketing that is used to promote any film rated by the Classification and Rating Administration, which is also a voluntary system. This includes 60,000 pieces of marketing each year including online trailers. The Advertising Administration takes every step to ensure that all advertising content is suitable for its intended audience. The goal is to give parents the same confidence in movie advertising that they have in the movie ratings system.

There are certain restrictions that are applicable to all advertising. For example, advertising may not misrepresent the content of the motion picture. All advertising that is approved falls into one of two categories: advertising approved without restrictions, or advertising approved with restrictions on its placement, including manner and/or time restrictions on its use, depending on the media being used to market the movie. The official motion picture site must include on its splash page the Full Rating Block and hyperlinks to www.mpaa.org and www.filmratings.com, as must any trailer for the motion picture exhibited on the Internet. The goal is to ensure suitability, transparency, and consistency.

One example of industry and self-regulation was of a review of an "Ironman 3" preview, which was rated PG-13 for "sci-fi action violence", and "brief suggestive content" and appeared during "SpongeBob SquarePants." This was an example of MPAA and CARU's referral agreement which prompts review of any instance when there is an advertisement for a film rated PG-13, R, or NC-17 in any medium primarily directed to children under 12. MPAA reviewed the issue at hand, and decided that the advertisement was acceptable because the content of the ad itself was not overtly sexual or violent, making it not inappropriate for younger audiences

(even though the MPAA rated the advertised movie as PG-13). According to the MPAA, it takes a holistic, case-by-case, view of a given ad's appropriateness, taking into account the ad itself, the movie it relates to, and the intended audience. The MPAA can impose an unspecified "remedy" or "review" if an ad for a movie is deemed unacceptable.[107]

The MPAA's definition of "advertising" is contained in Article II, § 1 of the MPAA's Advertising Administration Rules. Article III sets out the MPAA's advertising standards, and Article V describes violations and sanctions available.

DMA Self-Regulatory Program for Online Behavioral Advertising

The Direct Marketing Association ("DMA") guidelines apply to all advertisers, including non-members, and non-members were still subject to public naming (on the DMA website) and referral to the FTC for repeated violations. Most organizations referred to the FTC are ones that do not respond at all to contact efforts from the DMA. It was reported to the Workgroup that even non-members have been mostly compliant with the DMA guidelines through correcting mistakes they do make.

[107] Several Workgroup members were troubled by MPAA's practices in this regard. Specifically, they expressed the view that it is unfair and misleading to show advertisements for movies rated PG-13 or higher on children's media, even if the contents of those advertisements themselves do not contain material inappropriate for children under 13.

Proposed Recommendations Considered by the Workgroup

The Workgroup heard and considered several proposed recommendations for future action in Maryland on children's online privacy made by some of its members. The proposals – and resulting discussion among Workgroup members – are shared below. As mentioned in the Introduction, it is the intent of the Workgroup not to prescribe particular legislative outcomes. Accordingly, none of these proposals are being shared as formal recommendations of the entire Workgroup. As will be noted below, these proposals received a mixture of favor and disfavor by various Workgroup members.[108]

Proposed Recommendation 1: K-12 student privacy and cloud computing legislation

As discussed above, school systems and educators are increasingly turning to "cloud" services to store their data, including in Maryland, and there is a desire to ensure that this data is not used by the cloud service provider for commercial purposes. A proposal made to the Workgroup was to enact legislation that would prohibit cloud service providers from using any data they collect in Maryland under K-12 contracts for commercial purposes. This proposal does not prohibit use of cloud services by Maryland schools; it simply ensures that such cloud services are child-protective and do not facilitate the sale of information about children and minors.

Both Massachusetts and New York have introduced such legislation, *see* Appendix E, and it has been received favorably by both the education community and the business community. Some Workgroup member organizations had already testified in support of the proposed legislation. Workgroup members debated what such a law would mean for a teacher's cloud service account, and it was explained that the proposed law would not apply to teachers' personal cloud service accounts. It was also explained that, because the limitation is on "commercial purposes," such a law would not inhibit appropriate law enforcement uses of the data collected.

Proposed Recommendation 2: Legislation and/or guidance on encryption of data collected about children

A second proposal to the Workgroup was to require by law the encryption of information collected from and about children. Encryption of sensitive information is an industry best practice, incorporating the FTC-supported notion of "privacy by design." States like Massachusetts and Nevada already require encryption when personal information is transmitted over public networks or stored on portable media, and Maryland makes it unlawful for a person to require an individual to transmit her Social Security number over the Internet "unless the connection is secure or the individual's Social Security number is encrypted."[109] Such protection

[108] If readers of this Report would like more information about any aspect of the proposed recommendations described below, they may contact the Office of the Attorney General.
[109] Md. Code Ann., Com. Law § 14-3402(a)(3).

should be afforded to children's information, which is by nature a more sensitive category of information.

Some Workgroup members expressed the view that, because best practices of the Internet industry change frequently as technologies improve, encryption may not be the best standard to codify. "Reasonableness," the standard used in the COPPA Rule[110] and Maryland's Personal Information Protection Act,[111] is more workable. Additionally, an encryption requirement creates liability issues above and beyond those already created by federal and state laws pertaining to data security. It was suggested that the Workgroup support efforts to ensure the FTC and state attorneys general can adequately enforce existing obligations rather than create new ones.

Other Workgroup members felt that, at the very least, state-level guidance is needed on how to secure children's information in order to keep it private. The McDonald's case referenced above shows just how easy it is for a child's information to be found and possibly misused by others. Most Workgroup members agreed that guidance in this area would be useful.

***Proposed Recommendation 3*: Data minimization rules for Maryland children**

One principle for data privacy that operates in Europe and in the United States to a lesser extent[112] is data minimization. The proposed E.U. Data Protection Regulation and Directive, both currently under consideration by the European Parliament, would put in place new rules on data minimization, including requirements that personal data only be processed to the extent necessary, and only if the purposes fulfilled by the data processing in question cannot be fulfilled by means that do not involve personal data.[113] A proposal to the Workgroup was to enact data minimization rules for data collected about children and teens in Maryland.

Some members of the Workgroup pointed out that the preference of the Internet advertising industry is not to collect information about children. Others pointed out, however, that there are still many apps that do, and that some apps collect personal information unnecessarily.[114] The FTC's recent settlement with social network service Path over its collection of address information from children provides an example of over-collection of

[110] *See* Appendix C, 16 C.F.R. § 312.8.

[111] Md. Code Ann., Com. Law § 14-3503(a) ("To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.").

[112] *See, e.g.*, 15 U.S.C. § 6502(b)(1)(C) (provision of COPPA requiring the FTC to adopt rules that "prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity").

[113] EU Data Protection Directive, art. 7; EU Data Protection Regulation, art. 5; *see also* EU Data Protection Regulation, para. 30 (Processing of personal data "should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means.").

[114] *See* FED. TRADE COMM'N, STAFF REPORT, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 9-11 (Dec. 2012).

children's data.[115] Data minimization rules would prevent bad actors from over-collecting information from children and would not affect Industry members who already refrain from collecting such information.

A similar proposal was made that would require websites and online services to set children's privacy settings, by default, to collect the least amount of information necessary. In this way, children would not need to become online privacy experts in order to control how much information is being collected and shared about them online.

One challenge with this proposal is that some websites and online services, like Facebook, have as their central business model – and central consumer appeal – the sharing of information socially. For these sites, having the most privacy-protective setting be the default setting would undercut their functionality. For these sharing-oriented sites, a different approach may be needed.

All Workgroup members agreed that children and parents need more education on privacy settings so that they can play an active role in the minimization of the data they share online. *See* Proposed Recommendation 5 below.

***Proposed Recommendation 4*: Government-led education highlighting existing industry transparency and disclosure efforts for children**

Given the array of privacy tools already provided by Internet and app companies to children and their parents and guardians, more needs to be done to promote these tools and improve consumer literacy. Accordingly, the Workgroup received a proposal for the Maryland Office of the Attorney General to promote good industry efforts to empower consumer control over children's privacy.

It was explained to the Workgroup that the OAG is unable to endorse specific companies, given its consumer protection obligations vis-à-vis companies, but that it can work with associations and non-profit organizations on promoting transparency and greater privacy protection. It was also noted that these organizations may be in the best position to highlight good work by industry.

***Proposed Recommendation 5*: Encouragement of Maryland OAG participation in consumer education campaigns related to online privacy for children and teens**

Another proposal to the Workgroup was to implement an education campaign at the Maryland OAG on online privacy for children and teens. Other state attorney general's offices have taken on such campaigns in the past, sometimes in partnership with major industry groups like Facebook, with good success.

[115] FED. TRADE COMM'N, *Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, Feb. 1, 2013, *available at*: http://ftc.gov/opa/2013/02/path.shtm.

It was noted that the Maryland OAG already has an educational effort called "Community Leadership in Cyber Knowledge and Safety" ("CLICKS") that focuses on improving children's Internet safety, which includes protecting their online privacy.[116] The OAG agreed that more privacy-focused education like this would be helpful to consumers. Workgroup members pointed out that such efforts should cut across state agencies and not be confined to the Maryland OAG. Other government agencies that could undertake an educational campaign like this include the Governor's Office, Maryland State Department of Education, the Maryland Department of Public Safety and Correctional Services, the Maryland State Police, and the legislature.

All Workgroup members agreed that more education about children's online privacy is essential, and that more state resources should be devoted to this issue.

***Proposed Recommendation 6*: Maryland "eraser button" legislation**

Using California's recently-enacted "eraser button" legislation as a model, *see* Appendix E, the proposal was made to the Workgroup to recommend enactment of "eraser button" legislation in Maryland. Although the COPPA Rule requires operators of websites or online services to "retain personal information collected online from a child only as long as is reasonably necessary to fulfill the purpose for which the information was collected" (and to use reasonable measures when they delete it),[117] it does not offer children (or their parents or guardians) any right to delete information they have posted and then regretted sharing.

Workgroup members agreed that children should be able to delete content they have posted, though some said that most online businesses already allow this. Other Workgroup members pointed out that the legislation would be meant to ensure that all relevant businesses allow it; the worry is not with the blue-ribbon websites and online services but the more unscrupulous operations.

One Workgroup member expressed concern that this proposal would create conflicts with Section 230(c) ("Section 230") of the Communications Decency Act, 47 U.S.C. § 230, which immunizes providers of interactive computer services from civil liability for content posted by third parties. If a website now had the obligation to play an active role in the content posted by third parties, it would risk losing that Section 230 immunity. Other members noted that the immunity is not affected by content removal, but rather content creation. Furthermore, a central purpose of Section 230 is to immunize website operators from liability for taking down third party content that the website operator finds objectionable, even if the content is constitutional; Section 230(c)(2) reads, in relevant part:

[116] http://www.oag.state.md.us/clicks.htm.
[117] 16 C.F.R. § 312.10.

> No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to *restrict access to or availability of* material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, *whether or not such material is constitutionally protected*.

Thus, if a website deleted information provided by a child, it will not be subject to civil liability for that decision.

Another Workgroup member observed that a state law like this would invite a patchwork of state laws in an area – the Internet – that really requires federal, if not international, regulation, given its cross-border nature. A response to this observation was that the country's data breach notification protections are a patchwork of state laws and that system is working well.

Furthermore, a way to avoid state-by-state inconsistency would be for Maryland to enact "eraser button" legislation that mirrors California's. Lastly, states are often innovators – going above and beyond the protections offered by federal laws – and given that federal regulation of children's online privacy protection is quite slow, states need to be able to step in to protect this vulnerable population from predatory behavior.

The Workgroup was reminded that "eraser-button"-type regulations may be coming to the European Union, and so Internet companies that operate in the European market will need to find ways to comply with such a law as it is. Article 15 of the proposed Data Protection Regulation provides the obligation for Member States to ensure a person's right of access to his or her personal data, where access also includes data correction rights (Article 16) and erasure rights (Article 17).

***Proposed Recommendation 7*: Legislation limiting online advertising to children**

Again using recently-enacted California legislation as a model, the Workgroup heard a proposal for legislation limiting online advertising to children. Under this proposal, the legislature would prohibit advertisers from (1) advertising products online that it would be illegal for a child to purchase (e.g. alcohol, tobacco, firearms, obscene materials) on a website, online service, or app that is directed to children or a website, online service, and (2) advertising these products to a user that they have actual knowledge is a child and to whom they have specifically targeted advertising based on information about that child. Maryland already has some such restrictions for advertising in traditional media[118]; this change would extend those restrictions to the Internet.

Workgroup members noted that the process of advertising in magazines and other traditional media is different than it is for the Internet (with real-time bidding on ads for a myriad

[118] *See, e.g.*, Md. Code Ann., Crim. Law § 11-203 (obscenity advertising to minors); *id.* art. 2B § 21-105 (alcoholic beverage advertising to minors).

of sites). It is easier for an advertiser to know its audience when it places an ad in a magazine or during a commercial break for a television show.

Most Workgroup members did not object to ensuring that existing advertising prohibitions apply to online advertising, though most Workgroup members also agreed that a specific list of prohibited items, as was provided in California's law, would be preferable to broader prohibitions. Some Workgroup members objected to these prohibitions. In terms of the possible challenges of compliance, it was noted that the "actual knowledge" standard in the California law is helpful. Under the California law, websites/apps that have actual knowledge that a user is a minor are deemed in compliance "if the operator takes reasonable actions in good faith designed to avoid" the prohibited advertising. In addition, the California law permits child-directed websites and apps that have third-party advertising services to comply by notifying such third parties that the website or app is directed to minors; then, the advertising service is subject to the prohibited advertising provisions. Some members expressed concern that the California legislation violated Section 230 of the CDA, while others disagreed.

***Proposed Recommendation 8*: Legislation requiring notice/disclosures for online advertisements when they are knowingly targeted to children**

Workgroup members also reviewed a proposal to recommend legislation requiring online advertisements that are knowingly targeted to children to be labeled in some way as advertisements. As discussed above, native advertising, advergames, and other creative advertising strategies blur the lines between what is paid advertising content and what is non-advertising content. Indeed, the popular photo-sharing service Instagram indicated at one point that it would reserve the right *not* to distinguish between paid advertising content and other content, revising its Terms of Use to include this term: "You acknowledge that we may not always identify paid services, sponsored content, or commercial communications as such."[119] This proposal would ensure that children and their parents and guardians are better able to distinguish between the two types of content.

On television, most viewers know when programming content stops and paid advertising content starts because of the "commercial break" between the two. Moreover, where a broadcast station airs a program in return for payment, such as an infomercial, the station must disclose both that the program was paid for and by whom. This is because viewers are entitled to know by whom they are being persuaded.[120]

[119] Jenna Wortham & Nick Bilton, *What Instagram's New Terms of Service Mean for You*, N.Y. TIMES, Dec. 17, 2012, *available at*: http://bits.blogs.nytimes.com/2012/12/17/what-instagrams-new-terms-of-service-mean-for-you/?_r=0. Instagram later changed its approach. *See* Nicole Perlroth & Jenna Wortham, *Instagram Does an About-Face*, N.Y. TIMES, Dec. 20, 2012, *available at*: http://bits.blogs.nytimes.com/2012/12/20/instagram-does-about-face-reverts-to-previous-policy/.

[120] 47 U.S.C. § 317; *see also* 47 CFR § 73.1212. *Applicability of Sponsorship Identification Rules*, 40 FCC 141 (1963).

The Federal Communications Commission (FCC) has long recognized that children need special protections.[121] After conducting an extensive inquiry, the FCC found that "children—especially young children—have greater difficulty distinguishing programming from advertising than adults" and that basic fairness requires that a "clear separation be maintained between the program content and the commercial message."[122] To avoid taking unfair advantage of children, the FCC also prohibited "host-selling," the use of program characters to promote products,[123] and "program length commercials," a program associated with a product in which commercials for that product are aired.[124] Later, in response to the development of digital television, the FCC "tentatively conclude[d] that we should prohibit interactivity during children's programming that connects viewers to commercial matter unless parents 'opt in' to such services."[125]

This proposal would apply these concepts to Internet and mobile advertising directed to children. Given the multitude of ways in which advertising appears on the Internet and mobile devices, the requirement need not be a specific phrase or label, but rather an identifier of some sort. On Twitter, for example, the label "promoted Tweet" is used along with a distinctive icon; on Google, the label "Ad" is used along with other spatial cues (advertising appears both at the right-hand side of the screen and in at the top of the search results).

One Workgroup member expressed concern that such a law would make interactive computer services liable for the postings of third-party users, in violation of Section 230. However, it was pointed out that the proposed law would only apply to advertisers, not the websites that carry their advertisements.

A question that was raised was who would be liable if a user of a posting-driven website or online service, like Twitter or Facebook or Tumblr, were paid to promote a product and posted a photo of himself enjoying that product without disclosing that he was paid to promote it: Would the website on which he posted be liable for that nondisclosure? The response was no; this would be treated like endorsements. With endorsements, the liability is on the person making the endorsement, not the website on which that endorsement appears.[126]

Finally, a Workgroup member wondered how this law would operate, given that an advertiser might not know that their ad is being targeted to a Maryland consumer. The response was that the proposed law could be tailored to apply only to situations in which the advertiser has actual knowledge that it is targeting a consumer in Maryland and/or is collecting location information, like IP address information, prior to advertising. This raised a concern, expressed by a Workgroup member, that preventing such targeted advertising would require collecting additional information, when the goal should be to reduce information collected about children.

---

[121] FED. COMM. COMM'N, CHILDREN'S TELEVISION REPORT AND POLICY STATEMENT, 50 FCC 2d 1, 8-9 (1974).
[122] *Id.* at 15.
[123] *Id.* at 16.
[124] *Policies and Rules Concerning Children's Television Programming*, 6 FCC Rcd 2111, 2117-18 (1991).
[125] *Children's Television Obligations of Digital Television Broadcasters*, 19 FCC Rcd 22943, 22968 (2004).
[126] *See* 16 C.F.R. § 255.2 (FTC rules for enforcements); *see generally* FED. TRADE COMM'N, .COM DISCLOSURES (March 2013), *available at*: http://business.ftc.gov/sites/default/files/pdf/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

***Proposed Recommendation 9*: Legislation making a COPPA violation an unfair/deceptive trade practice under the Maryland Consumer Protection Act**

COPPA is enforceable by state attorneys general,[127] but only in federal courts, and only after a state attorney general has given written notice to the FTC and the FTC has declined to intervene.[128] Because lawyers in the Maryland OAG practice primarily in Maryland state courts, they would be more effective bringing COPPA cases in state proceedings. Accordingly, a proposal was made to make a violation of COPPA a violation of the state Consumer Protection Act. Because the Consumer Protection Act also includes a private right of action, it was suggested that such a change in law be clear that enforcement of a COPPA claim under the State Consumer Protection Act could only be done by the OAG.

This proposal was met with resistance by some members of the Workgroup, which support additional funding to train assistant attorneys general on federal court practice, but do not support their ability to bring federal cases in state courts.

***Proposed Recommendation 10*: Legislation updating Maryland's definitions of "personal information" to (a) meet COPPA definitions and (b) include other needed updates**

Maryland's main statutes defining "personal information" have not been updated since 2007 (the year the iPhone was introduced), and in that time the types of personal information that can be collected and shared about consumers has changed dramatically – e.g., precise geolocation information and fingerprints. The newly amended COPPA Rule updated the definition of "personal information" as it applies to children to include things like precise geolocation information,[129] photographs, and videos, and a proposal was made to update Maryland's statutory definitions as well in ways that protect children's privacy.

The proposal would peg the definitions of "personal information" in Maryland's Personal Information Protection Act to the definitions provided in the COPPA Rule. It would also update other definitions of "personal information" elsewhere in the Maryland Code.[130] The Workgroup expressed a preference for avoiding a separate state definition of "personal information" that is inconsistent with the one provided by the COPPA Rule.

[127] 15 U.S.C. § 6504.
[128] *Id.* §§ 6504(a)(2) and (b).
[129] *See supra* n.71.
[130] *See supra* n.36 and accompanying text.

Conclusion

This report is not intended to provide the General Assembly with a formal list of proposed legislative action, but rather to equip it with the information necessary to make informed decisions about how best to protect children's online privacy going forward. Thus, the report reflects the Workgroup's efforts over the past year to address each of the six issues assigned to it by the Maryland legislature and consider potential solutions proposed by the various Workgroup members.

Per legislative direction, the Workgroup was comprised of leaders in academia, industry, government, consumer advocacy, and children's health advocacy. This report's analysis of the six assigned issue areas reflects their contributions to research and discussion, as well as their sometimes differing views on the subject matter at hand. Similarly, the proposed recommendations listed in the report are a compilation of every recommendation proffered by Workgroup members. The inclusion of a proposed recommendation is not intended to imply an endorsement by the Workgroup. Rather, the list of proposed recommendations offers the General Assembly information about potential solutions considered, including the Workgroup's reactions to each.

Children today enjoy unprecedented access to the Internet, and their interactions with the online world continue to grow and evolve. While the Internet can be a powerful tool for education, socialization, and self-expression, it can also be a source of confusion and vulnerability for children. It is the hope of the Children's Online Privacy Workgroup that the General Assembly will find this report useful as it seeks to protect the privacy of Maryland's children while online and preserve the positive role the Internet plays in their growth and development.

Appendix A: Workgroup on Children's Online Privacy Protection
2013 Md. Laws, Chapter 246

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That

(a) The Office of the Attorney General shall convene and direct a Workgroup to examine issues relating to the protection of children's privacy while using the Internet and mobile applications ("children's online privacy"), including:

(1) the nature and extent of data collected about children through Internet–based and mobile application–based advertising ("online advertising");

(2) current and forthcoming federal and state regulation of children's online privacy and online advertising and associated data collection;

(3) the effects on children of online behavioral advertising, native advertising, social advertising, and other forms of online advertising;

(4) best practices used by the Internet industry and the mobile application industry to protect children's online privacy;

(5) best practices urged by consumer advocates, children's health advocates, and regulators to protect children's online privacy; and

(6) the effectiveness of voluntary standards as they relate to children's online privacy.

(b) (1) The Workgroup required under subsection (a) of this section shall include representatives of State government, industry leaders, members of the academic community studying children's online privacy and the effects of online advertising on children, consumer advocates, and children's health advocates.

(2) The Office of the Attorney General shall invite representatives of relevant federal agencies to participate in the Workgroup.

(c) On or before December 31, 2013, the Office of the Attorney General shall report to the Senate Finance Committee and House Economic Matters Committee, in accordance with § 2–1246 of the State Government Article, on the findings of the Workgroup and any resulting recommendations.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect June 1, 2013.

Approved by the Governor, May 2, 2013.

Appendix B: Children's Online Privacy Protection Act ("COPPA")
15 U.S.C. § 6501 *et seq.* (1998)

TITLE 15. COMMERCE AND TRADE
CHAPTER 91. CHILDREN'S ON-LINE PRIVACY PROTECTION

§ 6501. Definitions

In this title [15 USCS §§ 6501 *et seq.*]:

(1) Child. The term "child" means an individual under the age of 13.

(2) Operator. The term "operator"--

(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce--

(i) among the several States or with 1 or more foreign nations;

(ii) in any territory of the United States or in the District of Columbia, or between any such territory and--

(I) another such territory; or

(II) any State or foreign nation; or

(iii) between the District of Columbia and any State, territory, or foreign nation; but

(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(3) Commission. The term "Commission" means the Federal Trade Commission.

(4) Disclosure. The term "disclosure" means, with respect to personal information--

(A) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and

(B) making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting, through the Internet, or through--

(i) a home page of a website;

(ii) a pen pal service;

(iii) an electronic mail service;

(iv) a message board; or

(v) a chat room.

(5) Federal agency. The term "Federal agency" means an agency, as that term is defined in section 551(1) of title 5, United States Code.

(6) Internet. The term "Internet" means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control

Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(7) Parent. The term "parent" includes a legal guardian.

(8) Personal information. The term "personal information" means individually identifiable information about an individual collected online, including--

(A) a first and last name;

(B) a home or other physical address including street name and name of a city or town;

(C) an e-mail address;

(D) a telephone number;

(E) a Social Security number;

(F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or

(G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

(9) Verifiable parental consent. The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

(10) Website or online service directed to children.

(A) In general. The term "website or online service directed to children" means--

(i) a commercial website or online service that is targeted to children; or

(ii) that portion of a commercial website or online service that is targeted to children.

(B) Limitation. A commercial website or online service, or a portion of a commercial website or online service, shall not be deemed directed to children solely for referring or linking to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

(11) Person. The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

(12) Online contact information. The term "online contact information" means an e-mail address or another substantially similar identifier that permits direct contact with a person online.

§ 6502. Regulation of unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the Internet

(a) Acts prohibited.

(1) In general. It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).

(2) Disclosure to parent protected. Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under subsection (b)(1)(B)(iii) to the parent of a child.

(b) Regulations.

(1) In general. Not later than 1 year after the date of the enactment of this Act [enacted Oct. 21, 1998], the Commission shall promulgate under section 553 of title 5, United States Code, regulations that--

(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child--

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent--

(i) a description of the specific types of personal information collected from the child by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;

(C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(2) When consent not required. The regulations shall provide that verifiable parental consent under paragraph (1)(A)(ii) is not required in the case of--

(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;

(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;

(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request--

(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)--

(i) used only for the purpose of protecting such safety;

(ii) not used to recontact the child or for any other purpose; and

(iii) not disclosed on the site,

if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary--

(i) to protect the security or integrity of its website;

(ii) to take precautions against liability;

(iii) to respond to judicial process; or

(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

(3) Termination of service. The regulations shall permit the operator of a website or an online service to terminate service provided to a child whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.

(c) Enforcement. Subject to sections 1304 and 1306 [15 USCS §§ 6503 and 6505], a violation of a regulation prescribed under subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(d) Inconsistent State law. No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this title that is inconsistent with the treatment of those activities or actions under this section.

§ 6503. Safe harbors

(a) Guidelines. An operator may satisfy the requirements of regulations issued under section 1303(b) [15 USCS § 6502(b)] by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).

(b) Incentives.

(1) Self-regulatory incentives. In prescribing regulations under section 1303 [15 USCS § 6502], the Commission shall provide incentives for self-regulation by operators to implement the

protections afforded children under the regulatory requirements described in subsection (b) of that section.

(2) Deemed compliance. Such incentives shall include provisions for ensuring that a person will be deemed to be in compliance with the requirements of the regulations under section 1303 [15 USCS § 6502] if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of the regulations issued under section 1303 [15 USCS § 6502].

(3) Expedited response to requests. The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.

(c) Appeals. Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

§ 6504. Actions by States

(a) In general.

(1) Civil actions. In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 1303(b) [15 USCS § 6502(b)], the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to--

(A) enjoin that practice;

(B) enforce compliance with the regulation;

(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) Notice.

(A) In general. Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Commission--

(i) written notice of that action; and

(ii) a copy of the complaint for that action.

(B) Exemption.

(i) In general. Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(ii) Notification. In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(b) Intervention.

(1) In general. On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) Effect of intervention. If the Commission intervenes in an action under subsection (a), it shall have the right--

(A) to be heard with respect to any matter that arises in that action; and

(B) to file a petition for appeal.

(3) Amicus curiae. Upon application to the court, a person whose self-regulatory guidelines have been approved by the Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding.

(c) Construction. For purposes of bringing any civil action under subsection (a), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(d) Actions by the Commission. In any case in which an action is instituted by or on behalf of the Commission for violation of any regulation prescribed under section 1303, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that regulation.

(e) Venue; service of process.

(1) Venue. Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(2) Service of process. In an action brought under subsection (a), process may be served in any district in which the defendant--

(A) is an inhabitant; or

(B) may be found.

§ 6505. Administration and applicability of Act

(a) In general. Except as otherwise provided, this title [15 USCS §§ 6501 *et seq.*] shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 *et seq.*).

(b) Provisions. Compliance with the requirements imposed under this title [15 USCS §§ 6501 *et seq.*] shall be enforced under--

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a) of the Federal Reserve Act (12 U.S.C. 601 *et seq.* and 611 *et seq.*), by the Board; and

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;

(3) the Federal Credit Union Act (12 U.S.C. 1751 *et seq.*) by the National Credit Union Administration Board with respect to any Federal credit union;

(4) part A of subtitle VII of title 49, United States Code [49 USCS §§ 40101 *et seq.*], by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 *et seq.*) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and

(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) Exercise of certain powers. For the purpose of the exercise by any agency referred to in subsection (a) [subsection (b)] of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this title shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this title [15 USCS §§ 6501 *et seq.*], any other authority conferred on it by law.

(d) Actions by the Commission. The Commission shall prevent any person from violating a rule of the Commission under section 1303 [15 USCS § 6502] in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 *et seq.*) were incorporated into and made a part of this title. Any entity that violates such rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this title [15 USCS §§ 6501 *et seq.*].

(e) Effect on other laws. Nothing contained in the Act shall be construed to limit the authority of the Commission under any other provisions of law.

§ 6506. Review

Not later than 5 years after the effective date of the regulations initially issued under section 1303 [15 USCS § 6502], the Commission shall--

(1) review the implementation of this title, including the effect of the implementation of this title on practices relating to the collection and disclosure of information relating to children,

children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and

(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

Appendix C: COPPA Rule
16 C.F.R. § 312

TITLE 16 -- COMMERCIAL PRACTICES
CHAPTER I -- FEDERAL TRADE COMMISSION
SUBCHAPTER C -- REGULATIONS UNDER SPECIFIC ACTS OF CONGRESS
PART 312 -- CHILDREN'S ONLINE PRIVACY PROTECTION RULE

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, et seq.,) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;

(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(3) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and

(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(1) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(2) Authorizes any collection, use, and/or disclosure of the personal information.

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

Operator means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is collected or maintained on behalf of an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(1) A first and last name;

(2) A home or other physical address including street name and name of a city or town;

(3) Online contact information as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(5) A telephone number;

(6) A Social Security number;

(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is 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;

(8) A photograph, video, or audio file where such file contains a child's image or voice;

(9) Geolocation information sufficient to identify street name and name of a city or town; or

(10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the Web site or online service means:

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the Web site or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the Web site or online service;

(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, Web site, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);

(2) So long as the information collected for the activities listed in paragraphs (1)(i)-(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

Third party means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the Web site or online service; or

(2) A person who provides support for the internal operations of the Web site or online service and who does not use or disclose information protected under this part for any other purpose.

Web site or online service directed to children means a commercial Web site or online service, or portion thereof, that is targeted to children.

(1) In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(2) A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children.

(3) A Web site or online service that is directed to children under the criteria set forth in paragraph (1) of this definition, but that does not target children as its primary audience, shall not be deemed directed to children if it:

(i) Does not collect personal information from any visitor prior to collecting age information; and

(ii) Prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(4) A Web site or online service shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) General principles of notice. It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) Direct notice to the parent. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) Content of the direct notice to the parent-- (1) Content of the direct notice to the parent under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information). This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

(2) Content of the direct notice to the parent under § 312.5(c)(2) (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information). Where an operator chooses to notify a parent of a child's participation in a Web site or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information;

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the child's participation in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(3) Content of the direct notice to the parent under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times). This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and

(vi) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(4) Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety). This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(d) Notice on the Web site or online service. In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service. Provided

that: The operators of a Web site or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the Web site or online service are also listed in the notice;

(2) A description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and, the operator's disclosure practices for such information; and

(3) That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

§ 312.5 Parental consent.

(a) General requirements. (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) Methods for verifiable parental consent. (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or

(vi) Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(3) Safe harbor approval of parental consent methods. A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c) Exceptions to prior parental consent. Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child except as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts,

taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of its Web site or online service;

(ii) Take precautions against liability;

(iii) Respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or

(8) Where an operator covered under paragraph (2) of the definition of Web site or online service directed to children in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a Web site or online service, the operator of that Web site or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Data retention and deletion requirements.

An operator of a Web site or online service shall retain 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. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

§ 312.11 Safe harbor programs.

(a) In general. Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with

the Commission's Office of the Secretary. The Commission will publish in the Federal Register a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) Criteria for approval of self-regulatory program guidelines. Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) Request for Commission approval of self-regulatory program guidelines. A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) How the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) How the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) Reporting and recordkeeping requirements. Approved safe harbor programs shall:

(1) By July 1, 2014, and annually thereafter, submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of any disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section.

(e) Post-approval modifications to self-regulatory program guidelines. Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2) of this section. The statement required under paragraph (c)(4) of this section must describe how the proposed changes affect existing provisions of the guidelines.

(f) Revocation of approval of self-regulatory program guidelines. The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, by March 1, 2013, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) Operators' participation in a safe harbor program. An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to

initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

§ 312.12 Voluntary Commission Approval Processes.

(a) Parental consent methods. An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the Federal Register a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request; and

(b) Support for internal operations of the Web site or online service. An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for internal operations. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for internal operations, and an analysis of their potential effects on children's online privacy. The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the Federal Register a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

Appendix D: "Do Not Track Kids" Act
S. 1700 / H.R. 3481

A BILL
To amend the Children's Online Privacy Protection Act of 1998 to extend, enhance, and revise the provisions relating to collection, use, and disclosure of personal information of children, to establish certain other protections for personal information of children and minors, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.
This Act may be cited as the ''Do Not Track Kids Act of 2013''.

SEC. 2. FINDINGS.
Congress finds the following:

(1) Since the enactment of the Children's Online Privacy Protection Act of 1998, the World Wide Web has changed dramatically, with the creation of tens of millions of websites, the proliferation of entirely new media platforms, and the emergence of a diverse ecosystem of services, devices, and applications that enable users to connect wirelessly within an online environment without being tethered to a desktop computer.

(2) The explosive growth of the Internet ecosystem has unleashed a wide array of opportunities to learn, communicate, participate in civic life, access entertainment, and engage in commerce.

(3) In addition to these significant benefits, the Internet also presents challenges, particularly with respect to the efforts of entities to track the online activities of children and minors and to collect, use, and disclose personal information about them, including their geolocation, for commercial purposes.

(4) Children and teens are visiting numerous companies' websites, and marketers are using multimedia games, online quizzes, and mobile phone and tablet applications to create ties to children and teens.

(5) According to a study by the Wall Street Journal in 2010, websites directed to children and teens were more likely to use cookies and other tracking tools than sites directed to a general audience.

(6) This study examined 50 popular websites for children and teens in the United States and found that these 50 sites placed 4,123 cookies, beacons, and other tracking tools on the test computer used for the study.

(7) This is 30 percent greater than the number of such tracking tools that were placed on the test computer in a similar study of the 50 overall most popular websites in the United States, which are generally directed to adults.

(8) Children and teens lack the cognitive ability to distinguish advertising from program content and to understand that the purpose of advertising is to persuade them, making them unable to activate the defenses on which adults rely.

(9) Children and teens are less able than adults to understand the potential long-term consequences of having their information available to third parties, including advertisers, and other individuals.

(10) According to Common Sense Media and the Center for Digital Democracy, 90 percent of teens have used some form of social media, 75 percent have a social networking site, and 51 percent check their social networking site at least once a day.

(11) Ninety-one percent of parents and 91 percent of adults believe it is not okay for advertisers to collect information about a child's location from that child's mobile phone.

(12) Ninety-four percent of parents and 91 percent of adults agree that advertisers should receive the parent's permission before putting tracking software on a child's computer.

(13) Ninety-six percent of parents and 94 percent of adults expressed disapproval when asked if it is ''okay for a website to ask children for personal information about their friends''.

(14) Eighty-eight percent of parents would support a law that requires search engines and social networking sites to get users' permission before using their personal information.

(15) A Commonsense Media/Zogby poll found that 94 percent of parents and 94 percent of adults believe individuals should have the ability to request the deletion, after a specific period of time, of all of their personal information held by an online search engine, social networking site, or marketing company.

(16) According to a Pew/Berkman Center poll, 69 percent of parents of teens who engage in online activity are concerned about how that activity might affect their children's future academic or employment opportunities.

(17) Eighty-one percent of parents of teens who engage in online activity say they are concerned about how much information advertisers can learn about their children's online activity.

SEC. 3. ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.

(a) DEFINITIONS.—Section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501) is amended—

(1) by amending paragraph (2) to read as follows:

''(2) OPERATOR.—The term 'operator'—

''(A) means any person who, for commercial purposes, in interstate or foreign commerce, operates or provides a website on the Internet, online service, online application, or mobile application, and who—

''(i) collects or maintains, either directly or through a service provider, personal information from or about the users of such website, service, or application;

''(ii) allows another person to collect personal information directly from users of such website, service, or application (in which case the operator is deemed to have collected the information); or

''(iii) allows users of such website, service, or application to publicly disclose personal information (in which case the operator is deemed to have collected the information); and

''(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).'';

(2) in paragraph (4)—

(A) by amending subparagraph (A) to read as follows:

''(A) the release of personal information for any purpose, except where such information is provided to a person other than an operator who provides support for the internal operations of the website, online service, online application, or mobile application of the operator and does not disclose or use that information for any other purpose; and''; and

(B) in subparagraph (B), by striking ''website or online service'' and inserting ''website, online service, online application, or mobile application'';

(3) in paragraph (8)—

(A) by amending subparagraph (G) to read as follows:

''(G) information concerning a child or the parents of that child (including any unique or substantially unique identifier, such as a customer number) that an operator collects online from the child and combines with an identifier described in subparagraphs (A) through (G).'';

(B) by redesignating subparagraphs (F) and (G) as subparagraphs (G) and (H), respectively; and

(C) by inserting after subparagraph (E) the following new subparagraph:

''(F) information (including an Internet protocol address) that permits the identification of an individual, the computer of an individual, or any other device used by an individual to access the Internet or an online service, online application, or mobile application;'';

(4) by striking paragraph (10) and redesignating paragraphs (11) and (12) as paragraphs (10) and (11), respectively; and

(5) by adding at the end the following new paragraph:

‘‘(12) ONLINE, ONLINE SERVICE, ONLINE APPLICATION, MOBILE APPLICATION, DIRECTED TO CHILDREN.—The terms ‘online’, ‘online service’, ‘online application’, ‘mobile application’, and ‘directed to children’ shall have the meanings given such terms by the Commission by regulation. Not later than 1 year after the date of the enactment of the Do Not Track Kids Act of 2013, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that define such terms broadly enough so that they are not limited to current technology, consistent with the principles articulated by the Commission regarding the definition of the term ‘Internet’ in its statement of basis and purpose on the final rule under this title promulgated on November 3, 1999 (64 Fed. Reg. 59891).
The definition of the term ‘online service’ in such regulations shall include broadband Internet access service (as defined in the Report and Order of the Federal Communications Commission relating to the matter of preserving the open Internet and broadband industry practices (FCC 10–201, adopted by the Commission on December 21, 2010)).’’.

(b) ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.—Section 1303 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended—

(1) by striking the heading and inserting the following: ‘‘**ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.**’’;

(2) in subsection (a)—

(A) by amending paragraph (1) to read as follows:

‘‘(1) IN GENERAL.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).’’; and

(B) in paragraph (2)—

(i) by striking ‘‘of such a website or online service’’; and

(ii) by striking ‘‘subsection (b)(1)(B)(iii)’’ and inserting ‘‘subsection (b)(1)(C)(iii)’’; and

(3) in subsection (b)—

(A) by amending paragraph (1) to read as follows:

‘‘(1) IN GENERAL.—Not later than 1 year after the date of the enactment of the Do Not Track Kids Act of 2013, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to require an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child—

‘‘(A) to provide clear and conspicuous notice in clear and plain language of the types of personal information the operator collects, how the operator uses such information, whether the operator discloses such information, and the procedures or mechanisms the operator uses to ensure that personal information is not collected from children except in accordance with the regulations promulgated under this paragraph;

‘‘(B) to obtain verifiable parental consent for the collection, use, or disclosure of personal information of a child;

''(C) to provide to a parent whose child has provided personal information to the operator, upon request by and proper identification of the parent—

''(i) a description of the specific types of personal information collected from the child by the operator;

''(ii) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of personal information collected from the child; and

''(iii) a means that is reasonable under the circumstances for the parent to obtain any personal information collected from the child, if such information is available to the operator at the time the parent makes the request;

''(D) not to condition participation in a game, or use of a website, service, or application, by a child on the provision by the child of more personal information than is reasonably required to participate in the game or use the website, service, or application; and

''(E) to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.'';

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by striking ''paragraph (1)(A)(ii)'' and inserting ''paragraph (1)(B)''; and

(ii) in subparagraph (A), by inserting ''or to contact a different child'' after ''to recontact the child'';

(C) by amending paragraph (3) to read as follows:

''(3) CONTINUATION OF SERVICE.—The regulations shall prohibit an operator from discontinuing service provided to a child on the basis of refusal by the parent of the child, under the regulations prescribed under paragraph (1)(C)(ii), to permit the further use or maintenance in retrievable form, or future collection, by the operator of personal information collected from the child, to the extent that the operator is capable of providing such service without such information.''; and

(D) by adding at the end the following:

''(4) RULE FOR TREATMENT OF USERS OF WEBSITES, SERVICES, AND APPLICATIONS DIRECTED TO CHILDREN.—An operator of a website, online service, online application, or mobile application that is directed to children shall treat all users of such website, service, or application as children for purposes of this title, except as permitted by the Commission by a regulation promulgated under this title.''.

(c) ADMINISTRATION AND APPLICABILITY OF ACT.—Section 1306 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6505) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking '', in the case of'' and all that follows and inserting the following: ''by the appropriate Federal banking agency with respect to any insured depository institution (as such terms are defined in section 3 of such Act (12 U.S.C. 1813));''; and

(B) by striking paragraph (2) and redesignating paragraphs (3) through (6) as paragraphs (2) through (5), respectively; and

(2) by adding at the end the following new subsection:

''(f) TELECOMMUNICATIONS CARRIERS AND CABLE OPERATORS.—

''(1) ENFORCEMENT BY FTC.—Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), compliance with the requirements imposed under this title shall be enforced by the Commission with respect to any telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)).

''(2) RELATIONSHIP TO OTHER LAW.—To the extent that sections 222, 338(i), and 631 of the Communications Act of 1934 (47 U.S.C. 222; 338(i); 551) are inconsistent with this title, this title controls.''.

SEC. 4. TARGETED MARKETING TO CHILDREN OR MINORS.

(a) ACTS PROHIBITED.—It is unlawful for—

(1) an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child, to use, disclose to third parties, or compile personal information for targeted marketing purposes without verifiable parental consent; or

(2) an operator of a website, online service, online application, or mobile application directed to minors, or an operator having actual knowledge that personal information being collected is from a minor, to use, disclose to third parties, or compile personal information for targeted marketing purposes without the consent of the minor.

(b) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to implement this section.

SEC. 5. DIGITAL MARKETING BILL OF RIGHTS FOR TEENS AND FAIR INFORMATION PRACTICES PRINCIPLES.

(a) ACTS PROHIBITED.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to minors, or an operator having actual knowledge that personal information being collected is from a minor, to collect personal information from a minor unless such operator has adopted and complies with a Digital Marketing Bill of Rights for Teens that is consistent with the Fair Information Practices Principles described in subsection (b).

(b) FAIR INFORMATION PRACTICES PRINCIPLES.—

The Fair Information Practices Principles described in this subsection are the following:

(1) COLLECTION LIMITATION PRINCIPLE.—Except as provided in paragraph (3), personal information should be collected from a minor only when collection of the personal information is—

(A) consistent with the context of a particular transaction or service or the relationship of the minor with the operator, including collection necessary to fulfill a transaction or provide a service requested by the minor; or

(B) required or specifically authorized by law.

(2) DATA QUALITY PRINCIPLE.—The personal information of a minor should be accurate, complete, and kept up-to-date to the extent necessary to fulfill the purposes described in subparagraphs (A) through (D) of paragraph (3).

(3) PURPOSE SPECIFICATION PRINCIPLE.—The purposes for which personal information is collected should be specified to the minor not later than at the time of the collection of the information. The subsequent use or disclosure of the information should be limited to—

(A) fulfillment of the transaction or service requested by the minor;

(B) support for the internal operations of the website, service, or application, as described in section 312.2 of title 16, Code of Federal Regulations;

(C) compliance with legal process or other purposes expressly authorized under specific legal authority; or

(D) other purposes—

(i) that are specified in a notice to the minor; and

(ii) to which the minor has consented under paragraph (7) before the information is used or disclosed for such other purposes.

(4) RETENTION LIMITATION PRINCIPLE.—The personal information of a minor should not be retained for longer than is necessary to fulfill a transaction or provide a service requested by the minor or such other purposes specified in subparagraphs (A) through (D) of paragraph (3). The operator should implement a reasonable and appropriate data disposal policy based on the nature and sensitivity of such personal information.

(5) SECURITY SAFEGUARDS PRINCIPLE.—The personal information of a minor should be protected by reasonable and appropriate security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.

(6) OPENNESS PRINCIPLE.—

(A) IN GENERAL.—The operator should maintain a general policy of openness about developments, practices, and policies with respect to the personal information of a minor. The operator should provide each minor using the website, online service, online application, or mobile application of the operator with a clear and prominent means—

(i) to identify and contact the operator, by, a at minimum, disclosing, clearly and prominently, the identity of the operator and—

(I) in the case of an operator who is an individual, the address of the principal residence of the operator and an email address and telephone number for the operator; or

(II) in the case of any other operator, the address of the principal place of business of the operator and an email address and telephone number for the operator;

(ii) to determine whether the operator possesses any personal information of the minor, the nature of any such information, and the purposes for which the information was collected and is being retained;

(iii) to obtain any personal information of the minor that is in the possession of the operator from the operator, or from a person specified by the operator, within a reasonable time after making a request, at a charge (if any) that is not excessive, in a reasonable manner, and in a form that is readily intelligible to the minor;

(iv) to challenge the accuracy of personal information of the minor that is in the possession of the operator; and

(v) if the minor establishes the inaccuracy of personal information in a challenge under clause (iv), to have such information erased, corrected, completed, or otherwise amended.

(B) LIMITATION.—Nothing in this paragraph shall be construed to permit an operator to erase or otherwise modify personal information requested by a law enforcement agency pursuant to legal authority.

(7) INDIVIDUAL PARTICIPATION PRINCIPLE.—
The operator should—

(A) obtain consent from a minor before using or disclosing the personal information of the minor for any purpose other than the purposes described in subparagraphs (A) through (C) of paragraph (3); and

(B) obtain affirmative express consent from a minor before using or disclosing previously collected personal information of the minor for purposes that constitute a material change in practice from the original purposes specified to the minor under paragraph (3).

(c) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to implement this section, including regulations further defining the Fair Information Practices Principles described in subsection (b).

SEC. 6. ONLINE COLLECTION OF GEOLOCATION INFORMATION OF CHILDREN AND MINORS.

(a) ACTS PROHIBITED.—

(1) IN GENERAL.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or minors, or an operator having actual knowledge that geolocation information being collected is from a child or minor, to collect geolocation information from a child or minor in a manner that violates the regulations prescribed under subsection (b).

(2) DISCLOSURE TO PARENT OR MINOR PROTECTED.—Notwithstanding paragraph (1), neither an operator nor the operator's agent shall be held to be liable under any

Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of geolocation information under subparagraph (C)(ii)(III) or (D)(ii)(III) of subsection (b)(1).

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that require an operator of a website, online service, online application, or mobile application directed to children or minors, or an operator having actual knowledge that geolocation information being collected is from a child or minor—

(A) to provide clear and conspicuous notice in clear and plain language of any geolocation information the operator collects, how the operator uses such information, and whether the operator discloses such information;

(B) to establish procedures or mechanisms to ensure that geolocation information is not collected from children or minors except in accordance with regulations promulgated under this paragraph;

(C) in the case of collection of geolocation information from a child—

(i) prior to collecting such information, to obtain verifiable parental consent; and

(ii) after collecting such information, to provide to the parent of the child, upon request by and proper identification of the parent—

(I) a description of the geolocation information collected from the child by the operator;

(II) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of geolocation information from the child; and

(III) a means that is reasonable under the circumstances for the parent to obtain any geolocation information collected from the child, if such information is available to the operator at the time the parent makes the request; and

(D) in the case of collection of geolocation information from a minor—

(i) prior to collecting such information, to obtain affirmative express consent from such minor; and

(ii) after collecting such information, to provide to the minor, upon request—

(I) a description of the geolocation information collected from the minor by the operator;

(II) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of geolocation information from the minor; and

(III) a means that is reasonable under the circumstances for the minor to obtain any geolocation information collected from the minor, if such information is available to the operator at the time the minor makes the request.

(2) WHEN CONSENT NOT REQUIRED.—The regulations promulgated under paragraph (1) shall provide that verifiable parental consent under subparagraph (C)(i) of such

paragraph or affirmative express consent under subparagraph (D)(i) of such paragraph is not required when the collection of the geolocation information of a child or minor is necessary, to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

(3) CONTINUATION OF SERVICE.—The regulations promulgated under paragraph (1) shall prohibit an operator from discontinuing service provided to—

(A) a child on the basis of refusal by the parent of the child, under subparagraph (C)(ii)(II) of such paragraph, to permit the further use or maintenance in retrievable form, or future online collection, of geolocation information from the child by the operator, to the extent that the operator is capable of providing such service without such information; or

(B) a minor on the basis of refusal by the minor, under subparagraph (D)(ii)(II) of such paragraph, to permit the further use or maintenance in retrievable form, or future online collection, of geolocation information from the minor by the operator, to the extent that the operator is capable of providing such service without such information.

(c) INCONSISTENT STATE LAW.—No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this section that is inconsistent with the treatment of those activities or actions under this section.

SEC. 7. REMOVAL OF CONTENT.

(a) ACTS PROHIBITED.—It is unlawful for an operator of a website, online service, online application, or mobile application to make publicly available through the website, service, or application content or information that contains or displays personal information of children or minors in a manner that violates the regulations prescribed under subsection (b).

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that require an operator—

(A) to the extent technologically feasible, to implement mechanisms that permit a user of the website, service, or application of the operator to erase or otherwise eliminate content or information submitted to the website, service, or application by such user that is publicly available through the website, service, or application and contains or displays personal information of children or minors; and

(B) to take appropriate steps to make users aware of such mechanisms and to provide notice to users that such mechanisms do not necessarily provide comprehensive removal of the content or information submitted by such users.

(2) EXCEPTION.—The regulations promulgated under paragraph (1) may not require an operator or third party to erase or otherwise eliminate content or information that—

(A) any other provision of Federal or State law requires the operator or third party to maintain; or

(B) was submitted to the website, service, or application of the operator by any person other than the user who is attempting to erase or otherwise eliminate such content

or information, including content or information submitted by such user that was republished or resubmitted by another person.

(3) LIMITATION.—Nothing in this section shall be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

SEC. 8. ENFORCEMENT AND APPLICABILITY.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) IN GENERAL.—Except as otherwise provided, this Act and the regulations prescribed under this Act shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(2) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—Subject to subsection (b), a violation of this Act or a regulation prescribed under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(3) ACTIONS BY THE COMMISSION.—Subject to subsection (b), and except as provided in subsection (d)(1), the Commission shall prevent any person from violating this Act or a regulation prescribed under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, and any person who violates this Act or such regulation shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES.—Notwithstanding subsection (a), compliance with the requirements imposed under this Act shall be enforced as follows:

(1) Under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) by the appropriate Federal banking agency, with respect to an insured depository institution (as such terms are defined in section 3 of such Act (12 U.S.C. 1813)).

(2) Under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board, with respect to any Federal credit union.

(3) Under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation, with respect to any air carrier or foreign air carrier subject to such part.

(4) Under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of such Act (7 U.S.C. 226; 227)) by the Secretary of Agriculture, with respect to any activities subject to such Act.

(5) Under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration, with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—

(A) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this Act or

a regulation prescribed under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(i) enjoin that practice;

(ii) enforce compliance with this Act or such regulation;

(iii) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(iv) obtain such other relief as the court may consider to be appropriate.

(B) NOTICE.—

(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Commission—

(I) written notice of that action; and

(II) a copy of the complaint for that action.

(ii) EXEMPTION.—

(I) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this paragraph, if the attorney general determines that it is not feasible to provide the notice described in that clause before the filing of the action.

(II) NOTIFICATION.—In an action described in subclause (I), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(2) INTERVENTION.—

(A) IN GENERAL.—On receiving notice under paragraph (1)(B), the Commission shall have the right to intervene in the action that is the subject of the notice.

(B) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under paragraph (1), it shall have the right—

(i) to be heard with respect to any matter that arises in that action; and

(ii) to file a petition for appeal.

(3) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(4) ACTIONS BY THE COMMISSION.—In any case in which an action is instituted by or on behalf of the Commission for violation of this Act or a regulation prescribed under this Act, no State may, during the pendency of that action, institute an action under paragraph (1) against any defendant named in the complaint in the action instituted by or on behalf of the Commission for that violation.

(5) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) TELECOMMUNICATIONS CARRIERS AND CABLE OPERATORS.—

(1) ENFORCEMENT BY FTC.—Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), compliance with the requirements imposed under this Act shall be enforced by the Commission with respect to any telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)).

(2) RELATIONSHIP TO OTHER LAW.—To the extent that sections 222, 338(i), and 631 of the Communications Act of 1934 (47 U.S.C. 222; 338(i); 551) are inconsistent with this Act, this Act controls.

SEC. 9. RULE FOR TREATMENT OF USERS OF WEBSITES, SERVICES, AND APPLICATIONS DIRECTED TO CHILDREN OR MINORS.

An operator of a website, online service, online application, or mobile application that is directed to children or minors shall treat all users of such website, service, or application as children or minors (as the case may be) for purposes of this Act, except as permitted by the Commission by a regulation promulgated under this Act.

SEC. 10. DEFINITIONS.

(a) IN GENERAL.—In this Act:

(1) MINOR.—The term ‘‘minor’’ means an individual over the age of 12 and under the age of 16.

(2) TARGETED MARKETING.—The term ‘‘targeted marketing’’ means advertising or other efforts to market a product or service that are directed to a specific individual or device—

(A) based on the personal information of the individual or a unique identifier of the device; and

(B) as a result of use by the individual, or access by the device, of a website, online service, online application, or mobile application.

(b) TERMS DEFINED BY COMMISSION.—In this Act, the terms ‘‘directed to minors’’ and ‘‘geolocation information’’ shall have the meanings given such terms by the Commission by regulation. Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that define such terms broadly enough so that they are not limited to current technology, consistent with the principles articulated by the Commission regarding the definition of the term ‘‘Internet’’ in its statement of basis and purpose on the final rule under the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) promulgated on November 3, 1999 (64 Fed. Reg. 59891).

(c) OTHER DEFINITIONS.—The definitions set forth in section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501), as amended by section 3(a), shall apply in this Act, except to the extent the Commission provides otherwise by regulations issued under section 553 of title 5, United States Code.

SEC. 11. EFFECTIVE DATES.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), this Act and the amendments made by this Act shall take effect on the date that is 1 year after the date of the enactment of this Act.

(b) AUTHORITY TO PROMULGATE REGULATIONS.—
The following shall take effect on the date of the enactment of this Act:

(1) The amendments made by subsections (a)(5) and (b)(3)(A) of section 3.
(2) Sections 4(b), 5(c), 6(b), and 7(b).
(3) Subsections (b) and (c) of section 10.

(c) DIGITAL MARKETING BILL OF RIGHTS FOR TEENS.—Section 5, except for subsection (c) of such section, shall take effect on the date that is 180 days after the promulgation of regulations under such subsection.

Appendix E: Selected State Laws on Children's Online Privacy

California

California Online Privacy Protection Act of 2003
Cal. Bus. & Prof. Code §§22575-22579

22575.
(a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:
(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.
(4) Identify its effective date.

22576.
An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:
(a) Knowingly and willfully.
(b) Negligently and materially.

22577.
For the purposes of this chapter, the following definitions apply:
(a) The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

(1) A first and last name.
(2) A home or other physical address, including street name and name of a city or town.
(3) An e-mail address.
(4) A telephone number.
(5) A social security number.
(6) Any other identifier that permits the physical or online contacting of a specific individual.
(7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

(b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:

(A) Includes the word "privacy."

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

(c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner’s behalf or by processing information on behalf of the owner.

(d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

22578.

It is the intent of the Legislature that this chapter is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the posting of a privacy policy on an Internet Web site.

22579. This chapter shall become operative on July 1, 2004.

Privacy Rights for California Minors, Senate Bill 568

The people of the State of California do enact as follows:

SECTION 1.

Chapter 22.1 (commencing with Section 22580) is added to Division 8 of the Business and Professions Code, to read:

CHAPTER 22.1. Privacy Rights for California Minors in the Digital World

22580.
(a) An operator of an Internet Web site, online service, online application, or mobile application directed to minors shall not market or advertise a product or service described in subdivision (i) on its Internet Web site, online service, online application, or mobile application directed to minors.

(b) An operator of an Internet Web site, online service, online application, or mobile application:

(1) Shall not market or advertise a product or service described in subdivision (i) to a minor who the operator has actual knowledge is using its Internet Web site, online service, online application, or mobile application and is a minor, if the marketing or advertising is specifically directed to that minor based upon information specific to that minor, including, but not limited to, the minor's profile, activity, address, or location sufficient to establish contact with a minor, and excluding Internet Protocol (IP) address and product identification numbers for the operation of a service.

(2) Shall be deemed to be in compliance with paragraph (1) if the operator takes reasonable actions in good faith designed to avoid marketing or advertising under circumstances prohibited under paragraph (1).

(c) An operator of an Internet Web site, online service, online application, or mobile application directed to minors or who has actual knowledge that a minor is using its Internet Web site, online service, online application, or mobile application, shall not knowingly use, disclose, compile, or allow a third party to use, disclose, or compile, the personal information of a minor with actual knowledge that the use, disclosure, or compilation is for the purpose of marketing or advertising products or services to that minor for a product described in subdivision (i).

(d) "Minor" means a natural person under 18 years of age who resides in the state.

(e) "Internet Web site, online service, online application, or mobile application directed to minors" mean an Internet Web site, online service, online application, or mobile application, or a portion thereof, that is created for the purpose of reaching an audience that is predominately comprised of minors, and is not intended for a more general audience comprised of adults. Provided, however, that an Internet Web site, online service, online application, or mobile

application, or a portion thereof, shall not be deemed to be directed at minors solely because it refers or links to an Internet Web site, online service, online application, or mobile application directed to minors by using information location tools, including a directory, index, reference, pointer, or hypertext link.

(f) "Operator" means any person or entity that owns an Internet Web site, online service, online application, or mobile application. It does not include any third party that operates, hosts, or manages, but does not own, an Internet Web site, online service, online application, or mobile application on the owner's behalf or processes information on the owner's behalf.

(g) This section shall not be construed to require an operator of an Internet Web site, online service, online application, or mobile application to collect or retain age information about users.

(h) (1) With respect to marketing or advertising provided by an advertising service, the operator of an Internet Web site, online service, online application, or mobile application directed to minors shall be deemed to be in compliance with subdivision (a) if the operator notifies the advertising service, in the manner required by the advertising service, that the site, service, or application is directed to minors.

(2) If an advertising service is notified, in the manner required by the advertising service, that an Internet Web site, online service, online application, or mobile application is directed to minors pursuant to paragraph (1), the advertising service shall not market or advertise a product or service on the operator's Internet Web site, online service, online application, or mobile application that is described in subdivision (i).

(i) The marketing and advertising restrictions described in subdivisions (a) and (b) shall apply to the following products and services as they are defined under state law:

(1) Alcoholic beverages, as referenced in Sections 23003 to 23009, inclusive, and Section 25658.

(2) Firearms or handguns, as referenced in Sections 16520, 16640, and 27505 of the Penal Code.

(3) Ammunition or reloaded ammunition, as referenced in Sections 16150 and 30300 of the Penal Code.

(4) Handgun safety certificates, as referenced in Sections 31625 and 31655 of the Penal Code.

(5) Aerosol container of paint that is capable of defacing property, as referenced in Section 594.1 of the Penal Code.

(6) Etching cream that is capable of defacing property, as referenced in Section 594.1 of the Penal Code.

(7) Any tobacco, cigarette, or cigarette papers, or blunt wraps, or any other preparation of tobacco, or any other instrument or paraphernalia that is designed for the smoking or ingestion of tobacco, products prepared from tobacco, or any controlled substance, as referenced in Division

8.5 (commencing with Section 22950) and Sections 308, 308.1, 308.2, and 308.3 of the Penal Code.

(8) BB device, as referenced in Sections 16250 and 19910 of the Penal Code.

(9) Dangerous fireworks, as referenced in Sections 12505 and 12689 of the Health and Safety Code.

(10) Tanning in an ultraviolet tanning device, as referenced in Sections 22702 and 22706.

(11) Dietary supplement products containing ephedrine group alkaloids, as referenced in Section 110423.2 of the Health and Safety Code.

(12) Tickets or shares in a lottery game, as referenced in Sections 8880.12 and 8880.52 of the Government Code.

(13) Salvia divinorum or Salvinorin A, or any substance or material containing Salvia divinorum or Salvinorin A, as referenced in Section 379 of the Penal Code.

(14) Body branding, as referenced in Sections 119301 and 119302 of the Health and Safety Code.

(15) Permanent tattoo, as referenced in Sections 119301 and 119302 of the Health and Safety Code and Section 653 of the Penal Code.

(16) Drug paraphernalia, as referenced in Section 11364.5 of the Health and Safety Code.

(17) Electronic cigarette, as referenced in Section 119405 of the Health and Safety Code.

(18) Obscene matter, as referenced in Section 311 of the Penal Code.

(19) A less lethal weapon, as referenced in Sections 16780 and 19405 of the Penal Code.

(j) The marketing and advertising restrictions described in subdivisions (a), (b), and (c) shall not apply to the incidental placement of products or services embedded in content if the content is not distributed by or at the direction of the operator primarily for the purposes of marketing and advertising of the products or services described in subdivision (i).

(k) “Marketing or advertising” means, in exchange for monetary compensation, to make a communication to one or more individuals, or to arrange for the dissemination to the public of a communication, about a product or service the primary purpose of which is to encourage recipients of the communication to purchase or use the product or service.

22581.

(a) An operator of an Internet Web site, online service, online application, or mobile application directed to minors or an operator of an Internet Web site, online service, online application, or mobile application that has actual knowledge that a minor is using its Internet Web site, online service, online application, or mobile application shall do all of the following:

(1) Permit a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the user.

(2) Provide notice to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application that the minor may remove or, if the operator prefers, request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(3) Provide clear instructions to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application on how the user may remove or, if the operator prefers, request and obtain the removal of content or information posted on the operator's Internet Web site, online service, online application, or mobile application.

(4) Provide notice to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application that the removal described under paragraph (1) does not ensure complete or comprehensive removal of the content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(b) An operator or a third party is not required to erase or otherwise eliminate, or to enable erasure or elimination of, content or information in any of the following circumstances:

(1) Any other provision of federal or state law requires the operator or third party to maintain the content or information.

(2) The content or information was stored on or posted to the operator's Internet Web site, online service, online application, or mobile application by a third party other than the minor, who is a registered user, including any content or information posted by the registered user that was stored, republished, or reposted by the third party.

(3) The operator anonymizes the content or information posted by the minor who is a registered user, so that the minor who is a registered user cannot be individually identified.

(4) The minor does not follow the instructions provided to the minor pursuant to paragraph (3) of subdivision (a) on how the registered user may request and obtain the removal of content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(5) The minor has received compensation or other consideration for providing the content.

(c) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(d) An operator shall be deemed compliant with this section if:

(1) It renders the content or information posted by the minor user no longer visible to other users of the service and the public even if the content or information remains on the operator's servers in some form.

(2) Despite making the original posting by the minor user invisible, it remains visible because a third party has copied the posting or reposted the content or information posted by the minor.

(e) This section shall not be construed to require an operator of an Internet Web site, online service, online application, or mobile application to collect age information about users.

(f) "Posted" means content or information that can be accessed by a user in addition to the minor who posted the content or information, whether the user is a registered user or not, of the Internet Web site, online service, online application, or mobile application where the content or information is posted.

22582.
This chapter shall become operative on January 1, 2015.

SEC. 2.
The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

"Do Not Track" Act, Assembly Bill 370

The people of the State of California do enact as follows:

SECTION 1.
Section 22575 of the Business and Professions Code is amended to read:

22575.
(a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

(5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.

(6) Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service.

(7) An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.

Massachusetts

House No. 331

(filed on 1/15/2013)

An Act prohibiting service providers who offer cloud computing services to K-12 educational institutions from processing student data for commercial purposes.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

Section 1. Notwithstanding any general or special law to the contrary any person who provides a cloud computing service to an educational institution operating within the State shall process data of a student enrolled in kindergarten through twelfth grade for the sole purpose of providing the cloud computing service to the educational institution and shall not process such data for any commercial purpose, including but not limited to advertising purposes that benefit the cloud computing service provider.

New York

K12 Student Privacy and Cloud Computing Act, Assembly Bill 7243

AN ACT to amend the education law, in relation to enacting the "K12 student privacy and cloud computing act" to prohibit service providers who offer cloud computing services to primary and secondary educational institutions from processing student data for commercial purposes

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Short title. This act shall be known and may be cited as the "K12 student privacy and cloud computing act".

S 2. Legislative findings. The legislature hereby finds and declares:

1. Cloud computing services enable convenient, on-demand network access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction;

2. Cloud computing services offer tremendous potential to educational institutions in terms of helping consolidate technical infrastructure, reducing energy and capital costs, increasing collaboration through "anytime-anywhere" access to applications and information, and realizing efficiencies, network resilience, and flexible deployment; and

3. Cloud computing service providers hold the potential to invade the privacy of students by tracking students' online activities for commercial purposes, such as delivering behaviorally targeted advertising or otherwise improving advertising services that the service provider may offer in connection with or separate from the services it offers to the educational institution. In light of the foregoing, the legislature deems it necessary to ensure that when an educational institution engages a cloud computing service provider to process student data, that the service provider uses student data only for the benefit of the educational institution and does not use such data for the service provider's own commercial purposes.

EXPLANATION--Matter in CAPITALS is new; matter in brackets [ ] is old law to be omitted.

S 3. The education law is amended by adding a new section 755 to read as follows:

S 755. STUDENT PRIVACY AND CLOUD COMPUTING.

1. DEFINITIONS. FOR THE PURPOSES OF THIS SECTION, THE FOLLOWING TERMS SHALL HAVE THE FOLLOWING MEANINGS:

(A) "CLOUD COMPUTING SERVICE" SHALL MEAN A SERVICE THAT ENABLES CONVENIENT, ON-DEMAND NETWORK ACCESS TO A SHARED POOL OF CONFIGURABLE COMPUTING RESOURCES TO PROVIDE A STUDENT, TEACHER OR STAFF MEMBER ACCOUNT-BASED PRODUCTIVITY APPLICATIONS SUCH AS EMAIL, DOCUMENT STORAGE AND DOCUMENT EDITING THAT CAN BE RAPIDLY PROVISIONED AND RELEASED WITH MINIMAL MANAGEMENT EFFORT OR CLOUD COMPUTING SERVICE PROVIDER INTERACTION.

(B) "CLOUD COMPUTING SERVICE PROVIDER" SHALL MEAN AN ENTITY, OTHER THAN AN EDUCATIONAL INSTITUTION, THAT OPERATES A CLOUD COMPUTING SERVICE.

(C) "EDUCATIONAL INSTITUTION" SHALL MEAN ANY PUBLIC OR NONPUBLIC SCHOOL, CHARTER SCHOOL, SCHOOL DISTRICT OR BOARD OF COOPERATIVE EDUCATIONAL SERVICES SERVING STUDENTS IN GRADES KINDERGARTEN THROUGH TWELFTH GRADE.

(D) "PERSON" SHALL MEAN INDIVIDUAL, PARTNERSHIP, CORPORATION, ASSOCIATION, COMPANY OR ANY OTHER LEGAL ENTITY.

(E) "PROCESS" OR "PROCESSING" SHALL MEAN TO USE, ACCESS, MANIPULATE, SCAN, MODIFY, TRANSFORM, DISCLOSE, STORE, TRANSMIT, TRANSFER, RETAIN, AGGREGATE, OR DISPOSE OF STUDENT DATA.

(F) "STUDENT DATA" SHALL MEAN ANY INFORMATION OR MATERIALS IN ANY MEDIA OR FORMAT CREATED OR PROVIDED BY: (I) A STUDENT IN THE COURSE OF THE STUDENT'S USE OF THE CLOUD COMPUTING SERVICE; OR (II) AN EMPLOYEE OR AGENT OF THE EDUCATIONAL INSTITUTION THAT IS RELATED TO A STUDENT. IN EACH CASE THE TERM "STUDENT DATA" SHALL INCLUDE, BUT NOT BE LIMITED TO THE NAME, ELECTRONIC MAIL ADDRESS, POSTAL ADDRESS, PHONE NUMBER, EMAIL MESSAGE, WORD PROCESSING DOCUMENTS, UNIQUE IDENTIFIERS, METADATA, OF A STUDENT, OR ANY AGGREGATIONS OR DERIVATIVES THEREOF.

2. PROHIBITION ON THE USE OF STUDENT DATA. ANY PERSON WHO, WITH KNOWLEDGE THAT STUDENT DATA WILL BE PROCESSED, PROVIDES A CLOUD COMPUTING SERVICE TO AN EDUCATIONAL INSTITUTION, IS PROHIBITED FROM USING THAT CLOUD COMPUTING SERVICE TO PROCESS STUDENT DATA FOR ANY SECONDARY USES THAT BENEFIT THE CLOUD COMPUTING SERVICE PROVIDER OR ANY THIRD PARTY, INCLUDING, BUT NOT LIMITED TO, ONLINE BEHAVIORAL ADVERTISING, CREATING OR CORRECTING AN INDIVIDUAL OR HOUSEHOLD PROFILE PRIMARILY FOR THE CLOUD COMPUTING SERVICE PROVIDER'S OR ANY THIRD PARTY'S BENEFIT, THE SALE OF THE DATA FOR ANY COMMERCIAL PURPOSE, OR ANY OTHER SIMILAR COMMERCIAL FOR-PROFIT ACTIVITY; PROVIDED, HOWEVER, A CLOUD COMPUTING SERVICE MAY PROCESS OR

MONITOR STUDENT DATA SOLELY TO PROVIDE SUCH SERVICE TO THE EDUCATIONAL INSTITUTION AND MAINTAIN THE INTEGRITY OF SUCH SERVICE.

3. CERTIFICATION OF COMPLIANCE. ANY PERSON WHO ENTERS INTO AN AGREEMENT TO PROVIDE A CLOUD COMPUTING SERVICE TO AN EDUCATIONAL INSTITUTION MUST CERTIFY IN WRITING TO THE EDUCATIONAL INSTITUTION THAT IT SHALL COMPLY WITH THE TERMS AND CONDITIONS SET FORTH IN SUBDIVISION TWO OF THIS SECTION.

S 4. This act shall take effect on the first of November next succeeding the date on which it shall have become a law, provided that the commissioner of education and the board of regents are authorized to promulgate such rules and regulations as may be necessary for the timely implementation of this act on or before such effective date.