COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

RIN 3084-AB20

"COPPA Rule Review, 16 CFR Part 312, Project No. P104503"

December 23, 2011

By notice published on September 27, 2011, the Federal Trade Commission ("FTC") has proposed revisions to the agency's Children's Online Privacy Protection Act Rule ("COPPA Rule").[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that children's online privacy is adequately protected in response to changes in technology, business practices, and the use of the Internet.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. EPIC has a particular interest in children's online privacy. In 1995, EPIC wrote to then-FTC Commissioner Christine Varney, exposing industry practices that "ma[de] available to the public the names, addresses, ages and telephone numbers of young children."[2] We urged the FTC to investigate these business practices and to develop appropriate safeguards.

EPIC worked with the Center for Media Education ("CME"), which had published a groundbreaking study in 1996 on children's privacy, to develop COPPA and help ensure

[1] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59813 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312), http://www.ftc.gov/os/2011/09/110915coppa.pdf [hereinafter "COPPA Rule Review"].
[2] EPIC Letter to Christine Varney on Direct Marketing Use of Children's Data, EPIC, December 14, 1995 *available at* http://epic.org/privacy/internet/ftc/ftc_letter.html.

enactment. As the CME study found, young children cannot understand the potential effects of revealing their personal information; neither can they distinguish between substantive material on websites and the advertisements surrounding it. The targeting of children by marketers resulted in the release of huge amounts of private information into the market and triggered the need for COPPA.[3]

For the past 15 years, EPIC has pursued many of the critical online privacy issues concerning children.[4] EPIC has testified before lawmakers in support of strong privacy safeguards for children.[5] EPIC has also filed complaints with the Federal Trade Commission detailing unfair and deceptive trade practices that put children's privacy at risk.[6]

EPIC is also interested in emerging new technologies and practices that increase the amount of data collected about children. For example, EPIC filed several complaints[7] and a "friend of the court" brief concerning social networking sites' privacy practices.[8] These sites encourage users to make social connections online, but also build detailed profiles about users, and disclose personal information to third parties. In addition, EPIC has filed regulatory complaints and court documents concerning behavioral marketing practices—practices that expose Internet users' personal information to marketers, advertisers, and others without users'

[3] Center for Media Education, Web of Deception: Threats to Children from Online Marketing, 1996 *available at* http://www.cme.org/children/marketing/deception.pdf
[4] *See, e.g.*, EPIC, *supra* note 2.
[5] *Children's Privacy Protection and Parental Empowerment Act: Hearing on H.R. 3508 Before the Subcomm. On Crime of the H. Comm. On the Judiciary*, 104th Cong (1996), (statement of Marc Rotenberg, Executive Director, EPIC), available at https://epic.org/privacy/kids/EPIC_Testimony.html.
[6] EchoMetrix, Inc., __ F.T.C. __ (2009) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.
[7] Facebook, Inc., __ F.T.C. __ (2011) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.
[8] EPIC, *In re Facebook*, http://epic.org/privacy/inrefacebook/; EPIC, I*n re Google Buzz*, http://epic.org/privacy/ftc/googlebuzz/default.html; EPIC, *Harris v. Blockbuster*, http://epic.org/amicus/blockbuster/default.html.

knowledge.[9] These emerging practices affect many consumers, but children are particularly vulnerable.

These risks have already led the European Commission to propose regulations that increase privacy protections for users, especially children. The General Data Protection Regulation, due to be published in January 2012, notes that "[c]hildren deserve specific protection of their personal data" and recommends adopting the definition of "child" contained in the UN Convention on the Rights of the Child.[10] Thus, the regulation defines "child" as anyone under the age of 18.[11]

EPIC's experience with the recent Echometrix complaint underscores the need for strong Commission action to protect the online privacy of children. On September 29, 2009, EPIC filed a detailed complaint with the Commission alleging that Echometrix, a software company, was selling "parental control" software that was in fact monitoring children's online activity for marketing purposes.[12] As the company itself stated about its datamining service Pulse:

> Every single minute, Pulse is aggregating the Web's social media outlets such as chat and chat rooms, blogs, forums, instant messaging, and Web sites to extract meaningful user generated content from your target audience, the teens.[13]

The EPIC complaint asked the Commission to stop these practices, seek compensation for victims, and ensure that Echometrix's collection and disclosure practices comply with

---

[9] EPIC, *Privacy? Proposed Google/DoubleClick Merger*, http://epic.org/privacy/ftc/google/; EPIC, *Google Books Litigation*, http://epic.org/privacy/googlebooks/litigation.html.

[10] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, at 22, COM (2011), __ final (Nov. 29, 2011) *available at* http://ow.ly/d/qGV (draft).

[11] *Id.* at 38.

[12] Echometrix, Inc., __ F.T.C. __ (2009) (Complaint, Request for Investigation, Injunction, and Other Relief), http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf; *see also* EPIC, Echometrix, http://epic.org/privacy/echometrix/.

[13] Wendy Davis, Company Allegedly Uses Monitoring Software To Collect Data From Children, MediaPost News (Sept. 29, 2009), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=11442

COPPA. The Commission acknowledged receipt of the complaint, but waited over one year to complete an enforcement action against the company.[14]

Meanwhile, both the Department of Defense and the New York Attorney General took action against the company. The Department of Defense shared EPIC's concerns about this product, as it would place at risk children in military families. In a letter to Echometrix, the Manager of the Army and Air Force Exchange Service's Exchange Online Mall, which provides products and services for military families around the world, stated that

> "[i]t is very unfortunate that [EchoMetrix] did not inform me of this issue. Our customer's privacy and security is very important to us, and we trust our Mall partners to maintain the security of our customers. I have removed [EchoMetrix's] site, and it will stay offline until this matter with EPIC and the FTC is resolved."[15]

The New York Attorney General also understood the severity of the problem created by EchoMetrix and announced a settlement with the company.[16] The settlement required that EchoMetrix pay a $100,000 fine and prohibited the company from analyzing or sharing with third parties any private communications, information, or online activity to which they have access.[17]

I. The Scope of the Proposed Changes to the FTC's COPPA Rule

The agency proposes changes to 16 CFR §312 that govern the implementation of the Children's Online Privacy Protection Act. Such changes include: Definitions (Section 312.2); Notice (Section 312.4); Parental Consent (Section 312.5); Confidentiality, Security, and Integrity

[14] Press Release, Federal Trade Commission, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers (Nov. 30, 2010), http://www.ftc.gov/opa/2010/11/echometrix.shtm.
[15] Email from Matthew McCoy, AAFES to Kevin Sullivan and Jeffrey Supinsky, Echometrix, Oct. 14, 2009 *available at* http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf.
[16] Press Release, Office of the Attorney General, Cuomo Announces Agreement Stopping Software Company "EchoMetrix" from Selling Children's Private Online Conversations to Marketers (Sept. 15, 2010), http://www.ag.ny.gov/media_center/2010/sep/sep15a_10.html.
[17] *Id.*

of Personal Information Collected From Children (Section 312.8); Data Retention and Deletion Requirements (Section 312.10); Safe Harbors (Section 312.11).

EPIC supports the proposed COPPA Rule revisions. The proposed revisions update the COPPA Rule by taking better account of the increased use of mobile devices by users and of new data collection practices by businesses. The Commission could improve the proposed revisions by (1) clarifying the definitions of "Internet" and "Web site located on the Internet," (2) extending the definition of "personal information" to cover the combination of date of birth, gender, and ZIP code, and (3) Adding Data-Breach Notification Requirements. Improving the COPPA Rule would better protect the privacy of children online, thus fulfilling COPPA's mandate.[18] By improving the COPPA Rule, the Commission would also be serving the public interest.

I. The COPPA Rule is Essentially Sound, and has Benefitted Parents, Children, Other Consumers, and Operators Substantially

COPPA established a baseline legal recognition that the collection and use of information on young children should be treated with care and avoided if possible. This is a sensible approach that recognizes both the unique vulnerabilities of young children and the limitations of a self-regulatory approach, which would place an unreasonable burden on young minors to interpret privacy policies and make informed decisions about the disclosure and use of personal information.[19]

[18] *See* 15 U.S.C. §§ 6502, 6505 (2010).
[19] *An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the Sen. Comm. Commerce, Science, and Transportation*, 111th Cong. (Apr. 29, 2009) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center), at 3 [hereinafter Rotenberg Testimony], *available at* http://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

The Federal Trade Commission has used the statutory authority of COPPA to safeguard the interests of children in several high-profile cases. In 2006, the Commission fined the website Xanga $1 million for failing to obtain parental consent for children under 13 even though the site clearly targeted this population of users.[20] The Commission also fined UMG Recordings $400,000 for similar violations.[21] Most recently, the Commission settled a complaint against the website Skid-e-kids after the operator violated both the COPPA Rule and the website's own privacy policy by collecting personal information from approximately 5,600 children without obtaining prior parental consent.[22]

The proposed Rule includes several innovative provisions, including one that prohibits operators from conditioning a child's participation in an online activity on the provision of more information than is reasonably necessary to participate in that activity. Although the costs of the Rule to children, parents, and operators are negligible, the benefits are substantial. Children, who lack the maturity and sophistication to appreciate the privacy consequences of their online activities, receive a heightened level of protection compared to the privacy protections that other laws guarantee to adults. Parents benefit because operators are required to provide them with information about the kind of data collected about their children and the opportunity to prohibit further data collection or use. Operators benefit because the Rule, and the statute it accompanies, set forth guidelines enabling them to distinguish collection, storage, and disclosure of children's personal information that is permissible from that which is not permissible.

[20] Press Release, Federal Trade Commission, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule, (Sept. 7, 2006), http://www.ftc.gov/opa/2006/09/xanga.shtm.
[21] Press Release, Federal Trade Commission, UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. To Pay $75,000 to Settle COPPA Civil Penalty Charges, (Sept. 13, 2006), http://www.ftc.gov/opa/2004/02/bonziumg.shtm.
[22] Press Release, Federal Trade Commission, Operator of Social Networking Website for Kids Settles FTC Charges Site Collected Kids' Personal Information Without Parental Consent (Nov. 8, 2011), http://www.ftc.gov/opa/2011/11/skidekids.shtm; *see generally* Children's Privacy Enforcement, FTC, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

II. The COPPA Rule Amendments Improve the Existing Rule and Better Fulfill the Commission's Obligation to Enforce COPPA

COPPA requires that the Commission promulgate rules that require the operators of websites directed to children (1) obtain verifiable parental consent for the collection, use, or disclosure of such information, and (2) establish and maintain procedures to protect the confidentiality, security, and integrity of collected information.[23] In order to succeed in fulfilling this mandate, the Commission must regularly revise the COPPA Rule to account for changes in technology, business practices, and consumer behavior. The proposed COPPA Rule revisions are a well-reasoned and innovative approach to online privacy that respond to changes in the way children interact with the operators of web sites and online services.[24]

A. Section 312.2 ("Definitions")

The proposed regulation adds several new categories of information to the definition of "personal information" contained in 16 C.F.R. § 312.2: a "screen or user name," "persistent identifier" or "identifier that links the activities of a child across different Web sites or online services," "photograph, video, or audio file," and "Geolocation information." These new categories represent important improvements to the COPPA Rule.

First, the regulations consider screen and user names to be personal information, reflecting an understanding of the ease with which such information can be used to contact specific individuals. In many cases, consumers simply use their names to create user names.[25] Even when consumers create wholly fictitious user names, they often routinely reuse them on

[23] 15 U.S.C. §§ 6502, 6505 (2010).
[24] Somini Sengupta, *Update Urged on Children's Online Privacy*, N.Y. TIMES, (Sept. 15, 2011), https://www.nytimes.com/2011/09/16/technology/ftc-proposes-updates-to-law-on-childrens-online-privacy.html?_r=1.
[25] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, STANFORD CENTER FOR INTERNET & SOC'Y (Oct. 11, 2011 8:06am), http://cyberlaw.stanford.edu/node/6740.

different sites, and thus the user names may become linked across websites. In fact, "simple algorithms for linking user names could achieve pairwise precision and recall of over 70%" and companies such as Infochimps, Spokeo, and Google are already linking user names in their products.[26] Additionally, "combining data from multiple accounts often provides a sufficiently comprehensive mosaic to identify an individual."[27] A search for Stanford researcher Arvind Narayanan's user name, for example, "turned up his Y-Combinator Hacker News account, which includes his job and links to his personal website, blog, and Twitter account."[28] Finally, some websites, such as Quantcast, already include user name in their definition of personally identifiable information.[29]

The proposed regulations also consider persistent identifiers, such as cookies and IP addresses, to be personal information, regardless of whether they are paired with other identifying information. Again, this change reflects changes in technology and consumer behavior that have resulted in particular devices being increasingly associated with particular individuals. Furthermore, the rise of online behavioral advertising, the majority of which is accomplished through persistent identifiers, makes this addition to the COPPA Rule particularly important.

The new regulations include geolocation information within the definition of "personal information." This addition was necessitated by the increased use of mobile devices by children and the lack of clarity over whether such information was already covered under the existing Rule's inclusion of "street name and name of city or town." As with IP addresses and user

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

names, geolocation information can be used to track a particular device, which is usually linked to a particular individual.

B. Proposed Section 312.4 ("Notice") and Section 312 ("Parental Consent")

The proposed regulation streamlines the standards for web-site notices and specifically identifies the items which must be disclosed in the four types of direct notice available under the Rule. By simplifying the information contained in the web site notices, the proposed regulation helps ensure that such notices are more easily understood by consumers, most of whom are discouraged by the length and complexity of privacy policies.[30] Additionally, minimum standards make it easier for consumers to compare notices and determine which are more appropriate for themselves and their children.

The proposed regulation modifies 16 CFR § 312.5(b)(2) so that it includes new mechanisms for obtaining parental consent, such as electronically-scanned signed parental consent forms, while eliminating the method of sending a delayed confirmatory email after obtaining an address or telephone number from a parent—known as "email plus." This is a positive change, as email plus is unreliable because there is simply no effective way of determining whether the child has provided the parent's true email address or has instead created a fake email address.

The revision also correctly limits the method of obtaining parental consent through a financial transaction to the use of a credit card, modifying "transaction" with "monetary" to make this limitation clear. Alternative methods may not be as heavily regulated as more traditional systems. For example, the Electronic Funds Transfer Act (15 U.S.C. § 1691) (2006)

[30] *See, e.g.*, Janice Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, (June 2007), http://weis2007.econinfosec.org/papers/57.pdf.

and the Truth in Lending Act (15 U.S.C. § 1601) (2006) do not apply to PayPal, although they apply to credit card companies. As a result, the use of alternative methods to gain parental consent or payment remain inadvisable, although that may change as such methods come under stronger regulation.

C. Proposed Section 312.8 ("Confidentiality, Security, and Integrity of Personal Information Collected From Children")

The current regulation, 16 CFR § 312.8, states:

> The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

The proposed regulation adds several requirements to strengthen § 312.8's requirements:

> The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must take reasonable measures to ensure that any service provider or any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.

The new regulation enhances protection for the personal information of children. Web site operators continue to collect more information than necessary, and there have been several recent high-profile data breaches involving the personal data of consumers.[31] Furthermore, the burden of data security must rest primarily with the companies that collect personal information. Businesses that maintain consumer data are in a better position to safeguard the data. The data collectors are the "least cost avoiders" and can more efficiently protect the data in their

[31] For example, Sony's PlayStation Network was recently subject to a systemic attack by computer criminals, exposing the personal data of over 100 million consumers. *See* Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive data breach*, REUTERS (April 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

possession than could the data subjects who have transferred control over their personal information.[32]

Researchers have also shown that consumers face a variety of hurdles when making decisions that affect privacy.[33] These obstacles include (1) asymmetric information relative to the data holders that collect and use their information; (2) an inability to predict how non-sensitive information might be aggregated and analyzed to produce sensitive inferences; and (3) a host of cognitive and behavioral biases, such as a preference for instant gratification.[34] These cognitive hurdles are amplified in the case of children, who tend to be more impulsive and less capable of understanding the consequences of their online actions.[35] Because children's personal information is one of the most sensitive types of data collected by operators online, the security measures employed by those who handle this data are especially important.

D. Proposed Section 312.10 ("Data Retention and Deletion Requirements")

The proposed regulation includes a new data retention and deletion section, which will become 16 CFR § 312.10:

> 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.

---

[32] *See generally* GUIDO CALABRESI, THE COST OF ACCIDENTS (1970).
[33] *Understanding Consumer Attitudes About Privacy: Hearing before the Subcomm. On Commerce, Manufacturing and Trade of the H. Comm. on Energy and Commerce*, 112th Cong. (2011) (statement of Alessandro Acquisti, Professor, Heinz College, Carnegie Mellon University), http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Acquisti.pdf.
[34] *Id.* at 4-7.
[35] Center for Media Education, Web of Deception: Threats to Children from Online Marketing, 1996 *available at* http://www.cme.org/children/marketing/deception.pdf.

Data deletion requirements are an effective way to increase data security and thus work in tandem with the confidentiality, security, and integrity requirements contained in § 312.8. One of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks occur is to reduce the amount of sensitive personal information contained in the database. In fact, data minimization is one of the core tenets of the fair information practices that supply the basis for the Privacy Act of 1974. The Privacy Act directs agencies to maintain in their records only the minimum amount of information "relevant and necessary" to accomplish their purposes.[36]

Similar data minimization approaches have appeared in other federal privacy statutes. For example, the Video Privacy Protection Act requires businesses to "[d]estroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected . . . ."[37]

E. Proposed Section 312.11 ("Safe Harbors")

The current regulation, 16 CFR § 312.10, establishes a safe harbor for participants in Commission-approved self-regulatory programs. The proposed regulation moves the safe harbor provision to § 312.11 and requires operators to submit comprehensive information about their capability to run an effective safe harbor program, establishes greater Commission oversight of safe harbor programs, and requires safe harbor programs to submit periodic reports to the Commission:

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

[36] 5 U.S.C. § 552a(e)(1) (2010).
[37] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (Nov. 5, 1988), *codified at* 18 U.S.C. 2710.

(1) Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, the results of the independent assessment conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to requests by the Commission 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).

EPIC supports the regulation's requirement that operators participating in the safe-harbor program be required to undergo "independent assessment[s] of the subject operators' compliance" and to provide the Commission with the results of these audits. In the past, it was unclear whether the Commission had ever inspected the records of the safe harbor programs. The Commission could strengthen oversight further by requiring participants in the safe-harbor program to periodically re-apply for approval.

III. The Commission Should Further Improve the Proposed COPPA Rule by Defining Additional Terms, Extending the Definition of "Personal Information," and Adding Data-Breach Notification Requirements

Although the proposed regulation makes several significant improvements to the COPPA Rule, the Commission can further strengthen the rule by making several improvements. Improving the COPPA Rule would better protect the privacy of children online, thus fulfilling

COPPA's mandate.[38] By improving the COPPA Rule, the Commission would also be serving the public interest.

A. Definition of "Internet" and "Web site located on the Internet"

The Commission should define the key terms "Internet," and "Web site located on the Internet," and should extend the rule to cover text messaging services. The current regulation, 16 CFR § 312.2, defines "Internet" as:

> 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.

The Commission believes that the term "Internet" is defined "broadly enough to encompass many new technologies without the need for new statutory language."[39] However, the phrase "computer and telecommunications facilities" reflects an already-bygone time when "the Internet" was understood to be merely a network of computers. As such, it can be construed narrowly to exclude mobile devices and other applications that have only recently become "platform neutral," or capable of storing and transmitting data in the manner of a personal computer. This definition, therefore, should be modified so as to expressly acknowledge the convergence of technologies that is increasingly becoming a reality and to prevent future narrow constructions that would exclude new devices and applications.

The Commission understands the phrase "Web site located on the Internet," to "cover content that users can access through a browser on an ordinary computer or mobile," and the

[38] *See* 15 U.S.C. §§ 6502, 6505 (2010).
[39] COPPA Rule Review, at 59807.

term "online service" to include "mobile applications. . . [and] gaming platforms, voice-over-Internet protocol services, and Internet-enabled location based services."[40] The Commission's interpretations are desirable in that they ensure that COPPA remains relevant as more children access the Internet through mobile devices. Nevertheless, these understandings should be made explicit in the COPPA Rule so that the Rule's coverage is not jeopardized by a future Commission that is less inclined to enforce the Act.

Finally, the Commission should include short message services ("SMS") and multimedia messaging services ("MMS") within the Rule's coverage. The Commission has stated that it will "continue to assess emerging technologies to determine whether or not they constitute 'Web sites located on the Internet" or "online services" subject to COPPA's coverage."[41] Some panelists at the Commission's June 2, 2010 roundtable believe that mobile applications that enable users to send text messages between mobile devices without using the public Internet are not "online services."[42] However, COPPA refers to "a website located on the Internet *or an online service* . . ."[43] Because statutes should be construed "so as to avoid rendering superfluous" any statutory language,[44] the addition of the phrase "or an online service" indicates that COPPA was not limited to websites that collect information. Because "online" means "connected to a network or available from a network," [45] an "online service" can include text messages that are not Internet-based.

[40] *Id.*
[41] *Id.*
[42] *See Id.*
[43] 15 U.S.C. § 6501(2)(A) (2010) (emphasis added).
[44] *Sprietsma v. Mercury Marine*, 537 U.S. 51, 63 (2003).
[45] Webster's New World Pocket Internet Directory and Dictionary (Simon & Schuster, Inc., 1997) defines "online" as "connected to a network or available from a network."

Covering text messages will keep the COPPA Rule responsive to both the growing prevalence of mobile phones among children and the manner in which children use those phones. Fifty-four percent of children ages 8-12 will have cell phones within the next 3 years.[46] Furthermore, text messaging is rapidly becoming the preferred method of communication among children and teens with mobile phones.[47] Advertisers recognize that mobile devices are "the next great advertising medium,"[48] and as a result, they are increasingly taking advantage of these developments by targeting children in text messaging campaigns.[49] Thus, to account for the growing prevalence of mobile devices and text-message-based marketing, the Commission should extend COPPA's coverage to text messages.

B. Date of Birth, Gender, ZIP Code

The Commission should include the combination of date of birth, gender, and ZIP code in the proposed definition of personal information. This information, when combined, can also be used to personally identify individuals. Several studies have demonstrated that between 61 and 87 percent of the U.S. population can be uniquely identified by a combination of birth date, gender, and ZIP code.[50] Researchers at Carnegie Mellon University were able to use a person's date and state of birth to "identify in a single attempt the first five digits for 44 percent of deceased individuals who were born after 1988 . . . [and] to identify all nine digits for 8.5 percent

[46] Center on Media and Child Health, Cell Phones, http://cmch.tv/mentors/hotTopic.asp?id=70.
[47] Amanda Lenhart, *Teens, Cell Phones and Texting*, PEW RESEARCH CENTER (Apr. 20, 2010), http://pewresearch.org/pubs/1572/teens-cell-phones-text-messages.
[48] Kaiser Family Foundation, Daily Media Use Among Children and Teens Up Dramatically from Five Years Ago, Jan. 20, 2010, http://www.kff.org/entmedia/entmedia012010nr.cfm.
[49] *E.g.*, Amy Johannes, *McDonald's Serves Up Mobile Coupons in California*, Promo (Oct. 26, 2005), http://promomagazine.com/incentives/mcds_coupons_102605/.
[50] Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000) (87 percent individual identified based on birth date, gender, and ZIP code); Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y 77, 78 (2006) (61 percent of the population in 1990 and 63 percent in 2000 were uniquely identified by birth date, gender, and ZIP code).

of those individuals born after 1988 in fewer than 1,000 attempts."[51] Because the Commission's reason for including screen and user names, IP addresses, and geolocation information was that such information can allow operators to track and communication with specific individuals,[52] there is no principled basis for not also included a combination of date of birth, gender, and ZIP code within the Rule's definition of "personal information."

C. Data-Breach Notification

The regulation should also contain data breach notification requirements that require operators to notify parents within 48 hours whenever a breach occurs at a database containing the personal information of children. EPIC previously testified before the House Commerce Committee in support of the SAFE Data Act's 48-hour requirement for breach notification.[53] Short time periods require companies to respond quickly when there is a problem and allow parents to react more quickly and take preventative or mitigating actions.

IV. Conclusion

EPIC supports the proposed COPPA Rule revisions. The proposed revisions update the COPPA Rule by taking better account of the increased use of mobile devices and the new online information collection ecosystem. By incorporating the changes suggested above, the Commission can further strengthen the rule and ensure that children's online privacy is adequately protected in response to changes in technology, business practices, and the use of the Internet.

---

[51] Alessandro Acquisti and Ralph Gross, *Predicting Social Security numbers from public data*, 106 PNAS 10975, 10977-78 (2009), http://www.heinz.cmu.edu/~acquisti/ssnstudy/.
[52] *See* COPPA Rule Review, at 59810-59813.
[53] *See Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce*, 112th Cong. (2011) (statement of Marc Rotenberg, Executive Director, EPIC), http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

David Jacobs
EPIC Consumer Protection Fellow

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)
jacobs@epic.org

December 23, 2011