COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
THE FEDERAL TRADE COMMISSION
"2010 Children's Online Privacy Protection Act Rule Review"
FTC Matter No. P104503
July 9, 2010

The issue of children's online privacy remains highly relevant for consumers today. In the ten years since COPPA first went into effect, social networking participation has increased dramatically, especially among younger users of the Internet; mobile devices with location tracking capabilities have become popular amongst all users; and personally identifiable information has become a powerful economic tool for websites.

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

We are also interested in emerging technologies and practices that increase the amount of data collected about children. For example, EPIC filed several complaints and a "friend of the court" brief concerning social networking sites' privacy practices.[1] 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' knowledge.[2] These emerging practices affect many consumers, but children are particularly vulnerable.

EPIC's Comments and Recommendations

1. *There is a continuing need for the COPPA Rule, but recent technological developments have undermined the benefits of the Rule as it is currently promulgated.*

The need for the COPPA Rule has become increasingly urgent in light of new business practices and recent technological developments, such as social networking sites and mobile devices.[3] While the Rule does not contain any language that needs to be removed; some existing

---

[1] EPIC, *In re Facebook*, http://epic.org/privacy/inrefacebook/; EPIC, *In re Google Buzz*; http://epic.org/privacy/ftc/googlebuzz/; EPIC, *Harris v. Blockbuster*, http://epic.org/amicus/blockbuster/.
[2] EPIC, *Privacy? Proposed Google/DoubleClick Merger*, http://epic.org/privacy/ftc/google/; EPIC, *Google Books Litigation*, http://epic.org/privacy/googlebooks/litigation.html.
[3] *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,

provisions need to be strengthened and some new provisions need to be added. Children and teenagers represent a large percentage of the overall demographic of users of these services,[4] and the companies that operate or market these technologies have been resorting to increasingly deceptive means of collecting and storing children's personal information and disclosing this information to third parties.[5] The explosion in the use of social networking sites and mobile devices, particularly by children and teenagers, calls for the expansion of the COPPA Rule. Operators of social networking sites and companies that manufacture and market mobile devices have recently been engaging in new and troubling information-collecting and information-disclosing practices that the Rule as currently promulgated does not anticipate.

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. Specifically, § 312.7 of the rule prohibits operators from conditioning a child's participation in an online activity on the child's disclosure of more personal information than is reasonably necessary to participate in that activity.[6] Parents benefit because operators are required to provide to them upon their request: "(1) a description of the specific types of personal information collected from children; (2) the opportunity to refuse to permit the further use or collection of personal information from the child and to direct the deletion of the information; and (3) a means of reviewing any personal information collected from the child."[7] 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. These guidelines, however, can and should be improved so as to take account of opaque disclosure practices by social networking sites, locational tracking of mobile devices, and other troubling practices that have surfaced since the Rule was last reviewed.[8]

2. The Rule has benefitted parents, children, other consumers, and operators substantially.

Overall, COPPA has helped to establish a general understanding 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 the burden on minors to interpret privacy policies and make informed decisions about the disclosure and use of personal information.[9] The Rule includes several innovative provisions, including one that prohibits

---

Director, Electronic Privacy Information Center), at 2-5 [hereinafter Rotenberg Testimony], *available at* http://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

[4] *Id.*

[5] *Id.*

[6] 16 C.F.R. § 312.7 (2006).

[7] *Id.*

[8] *See* Rotenberg Testimony, *supra* note 3, at 4.

[9] *Id.* at 3.

operators from conditioning a child's participation in an online activity on the child's providing more information than is reasonably necessary to participate in that activity.[10]

The Rule has not imposed any costs on children, parents, or other consumers, but its adequacy has suffered recently in light of changes in business practices. The definitions in § 312.2 should be changed to take account of recent developments in the last five years, including social networking sites, mobile devices, and locational tracking. The Commission should require minimum standards in the delivery of notice requirements set forth in § 312.4. The Commission should add a provision to § 312.5(b)(2) expressly enumerating the delivery of a signed consent form in PDF format as an acceptable mode of notice delivery.

The Rule, furthermore, has effectively held operators to higher standards of privacy protection in the case of users who are 13 years old or younger. It has provided benefits to operators that more than compensate for whatever minimal costs economic or otherwise, it imposes on them.

3. The Rule should be structured to encourage state initiatives that protect children's privacy, rather than preempt state laws.

The COPPA rule provides an important baseline for privacy protection. But states should have the freedom to establish stronger protections and to develop innovative approaches to online privacy so as to better protect children's personal information in today's digital environment.

It would be a mistake for the COPPA rule to be structured so as to preempt state laws. While businesses will prefer a single national standard, privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. Indeed, state lawmakers have demonstrated a willingness to experiment with different approaches to better protect children.[11] This approach to consumer protection is based upon our federalism form of government, which allows the states to experiment with new legislative approaches to emerging issues; Louis Brandeis, the famous Supreme Court Justice, noted that the states are properly seen as "laboratories of democracy."[12] This view reflects the belief that there should be experimentation in regulatory approaches.

The COPPA rule should set a floor, not a ceiling, for children's privacy protection in the United States. If the Rule preempts state laws, states will be unable to develop new, effective

[10] *Id.*
[11] *E.g.* Illinois' Child Privacy Protection and Parental Empowerment Act (325 ILCS 17/1-20) (applying online privacy protections to children up to the age of 16, as contrasted with COPPA's protection of children up to the age of 13); California's Online Privacy Protection Act (Cal. Bus. and Prof. Code §§ 22575-22579) (applying online privacy protections to all websites, as contrasted with COPPA's application against sites that target children); Maine's Act to Prevent Predatory Marketing Practices Against Minors (10 MRSA § 1055) (prohibiting offline as well as online communications with minors, as opposed to COPPA's focus on online communications).
[12] *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932).

legislation that may respond more expeditiously to rapidly changing technologies.

4. The Rule currently places the burden on parents and teenagers to determine the standards of operators' notices.

At present, the Rule requires website operators to place notices on their websites describing their information practices.[13] While it is important for operators to make clear theur practices, such privacy notices are not particularly effective. The Rule places the burden on consumers to read individual notices for each site they use and determine the levels of privacy protections. Several studies have shown that consumers find privacy policies difficult to interpret.[14] Therefore, the information practice notices currently used may not be helpful to consumers in deciding which websites to view.

By incorporating minimum standards for operator notices into the Rule, the FTC can more effectively regulate websites by requiring operators to explain their information practices in language that consumers can more easily understand. Additionally, minimum standards that apply to all operators will make it easier for consumers to compare notices and determine which are more appropriate for themselves and their children.

5. Operators continue to collect more data from their users than necessary and the FTC must enforce COPPA more rigorously.

Although the FTC has had some success in pursuing enforcement actions under COPPA,[15] the agency has not sufficiently upheld its obligations under the statute.[16] Operators continue to make headlines by collecting more data than necessary, failing to adequately protect user privacy, and insufficiently notifying consumers (and more specifically parents) of their practices as they collect information.[17]

As a result, operators who target users who fall under the COPPA Rule are not adequately conforming with the Rule. By strengthening the definition of personally identifiable information (discussed *infra* at 7(d)) and pursuing enforcement actions more swiftly, the FTC can more effectively uphold the Congressional intent behind COPPA.

The Echometrix incident provides a clear example of why the FTC must enforce COPPA more rigorously. EPIC filed a complaint with the FTC regarding Echometrix, a company that sold "parental control" software that actually gathered data on children for marketing purposes.

---

[13] 16 C.F.R. § 312.4 (2006).
[14] *See, e.g.*, JANICE TSAI ET AL., THE EFFECT OF ONLINE PRIVACY INFORMATION ON PURCHASING BEHAVIOR: AN EXPERIMENTAL STUDY (unpublished working paper, *available at* http://weis2007.econinfosec.org/papers/57.pdf).
[15] FTC, *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.
[16] Rotenberg Testimony, *supra* note 3, at 5-7.
[17] *See, e.g.*, Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 12, 2010, at B8; Antone Goncalves, *Twitter, Feds Settle Security Charges*, INFORMATIONWEEK, June 25, 2010, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=225701450.

The FTC failed to respond to EPIC's complaint, but the Department of Defense prevented the company from selling the software to military families after reaching conclusions about the software's privacy violations similar to EPIC's.

The FTC has to date failed to explain why it did not take action in the Echometrix matter, despite the company's plain violation of COPPA and the Department of Defense's quick action to bar sales of the product. This episode exemplifies the deficiencies in the FTC's current approach to enforcing COPPA.

6. *Alternative methods of payment and authentication currently do not meet the requirements of the Rule, although they may in future.*

The FTC has suggested that alternative methods of authentication and payment may meet the standards described in the Rule.. Alternative methods may not be as heavily regulated as more traditional systems.[18] As a result, the use of alternative methods in gaining parental consent or payment remain inadvisable, although that may change as such methods come under stronger regulation.

7. *Overall, the definitions set forth in § 312.2 of the Rule accomplish this goal. However, there are a few areas where existing language can be strengthened or new language can be added in light of technological developments that have occurred since the Rule was last reviewed.*

The definitions in § 312.2 are clear, but they are not entirely appropriate, given recent technological developments.

a. *The Commission should modify the definitions of "collects or collection" and "disclosure" to take into account online technologies and Internet activities and features that have emerged since the Rule was enacted and that may emerge in the future.*

There is growing concern that companies are manipulating their privacy policies and privacy settings of users to confuse and frustrate users so that more personal information will be revealed. EPIC raised this concern in a petition filed with the Federal Trade Commission last December concerning the business practices of Facebook.[19] Also, the definition of "collects or collection" is ambiguous with regard to children's personal information that is acquired offline but that is uploaded, stored, or distributed to third parties by operators. That definition reads as follows:

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

[18] For example, the Electronic Funds Transfer Act (15 U.S.C. § 1691) (2006) and the Truth in Lending Act (15 U.S.C. § 1601) (2006) do not apply to PayPal, although they apply to credit card companies.
[19] Rotenberg Testimony, *supra* note 3, at 4 (citing EPIC, *In re Facebook*, http://epic.org/privacy/inrefacebook/).

(a) Requesting that children submit personal information online;

(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or

(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.[20]

Although the prefatory language contains the words "by any means" and "including but not limited to," none of the three enumerated examples expressly refer to the acquisition by an operator of children's personal information offline that is then uploaded, stored, or disclosed to third parties. One example of this is use of RFID technology for identity documents that makes it possible to track and record the location of children.[21]

The definition of "disclosure," moreover, needs to be strengthened in order to address the opaque manner in which social networking sites like Facebook share information with third parties. On the one hand, there is a great deal of transparency when users are able to see what they post and to make decisions about who should have access. On the other, the transfer of user data to application developers and now to web sites is much harder for users to observe and control.[22]

b. The Commission should exercise the utmost caution in modifying the definition of "deletes" so as to more expressly include the use of automated systems whereby where the operator "deletes" all individually identifiable information from postings by children before they are made public and deletes such information from the operator's records.

Unlawful disclosure of children's personal information under COPPA must remain a strict liability infringement. If an operator chooses to implement an automated system, and that system fails, the operator should not be able to claim any "safe harbor" immunity from enforcement by the Commission for the information it has inadvertently disclosed, simply because it uses an automated system.

c. The recent development of technologies such as mobile communications, interactive television, interactive gaming, and other similar interactive media call for changes to the Act's definition of "Internet."

[20] 16 C.F.R. § 312.2 (2006).
[21] *See* Rotenberg Testimony, *supra* note 3, at 9.
[22] *Id.* at 4.

In the past five years, the use of smart phones and other mobile devices has exploded, and children and teenagers have been a key demographic in this trend.[23] Recently, there have been a number of media reports that companies like Apple, which market mobile devices, have been tracking the location of users.[24]

The Rule as currently promulgated does not anticipate this development. Section 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.[25]

Yet today, and increasingly in the future, hitherto separate and distinct communications technologies will "converge," and an ever-expanding list of the items Americans use in their daily lives will go "online."[26] 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.

d. The items currently enumerated as "personal information" need to be clarified or modified in order for them to remain consistent with the Act.

---

[23] *See* Amanda Lenhart et al., *Social Media and Mobile Internet Use among Teens and Young Adults*, PewInternet (2010), *available at* http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[24] *E.g.,* Jennifer Valentino-DeVries, *Apple Changes Privacy Policy to Collect Location Data*, WALL ST. J., June 22, 2010, *available at* http://blogs.wsj.com/digits/2010/06/22/apple-changes-privacy-policy-to-collect-location-data/; Nick Saint, *WARNING: Check-in Apps Share Your Location With More People Than You Think,* S F. CHRON., June 30, 2010, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2010/06/30/businessinsider-warning-check-in-apps-are-sharing-your-location-with-more-people-than-you-think-2010-6.DTL; Tom Krazit*, Google Mobile Apps Collect Wi-Fi Location Data*, CNET, June 29, 2010, *available at* http://news.cnet.com/8301-30684_3-20009223-265.html.

[25] 16 C.F.R. 312.2 (2006) (emphasis added).

[26] For a more in-depth discussion of the "convergence" trend, see Daniel Lyons, *Technology Convergence and Federalism: Who Should Decide the Future of Telecommunications Regulation?*, 43 U. MICH. J.L REFORM 383 (2010); DongBack Seo & Mostafa Hashem Sherif, *Some Implications of an Overly Used Word: Convergence*, 4 INT'L J. TECH. MARKETING 316 (2009); N. Busis, *Mobile Phones to Improve the Practice of Neurology*, 28 NEUROLOGIC CLINICS 395 (2009); Satish Narayana Srirama et al., *Scalable Mobile Web Service Discovery in Peer to Peer Networks*, *available at* http://math.ut.ee/~srirama/publications/iciw08.pdf.

The scope of "personal information," as defined in § 312.2[27] of the Rule, should be expanded so as to expressly cover certain categories of information that have emerged in the wake of recent technological developments and that were not therefore anticipated in 2005 when the FTC last reviewed the Rule. That definition, as currently promulgated, reads as follows:

> 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 or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;
>
> (d) A telephone number;
>
> (e) A Social Security number;
>
> (f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or
>
> (g) 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.

Subsection (g) is a catch-all provision that, in theory, may cover the mobile web and location-based services that have come into common use in the past few years, particularly by children and teenagers.[28] However, current pervasiveness of these technologies necessitates that locational information derived from them where children are involved be expressly enumerated in a separate subsection of the "personal information" definition of § 312.2 of the COPPA Rule.

e. Section 1302(8)(F) of the Act provides the Commission with discretion to include in the definition of "personal information" any identifier that it determines would permit the physical or online contacting of a specific individual. Operators, including network advertising companies, have the

[27] 16 CFR § 312.2(a)-(g) (2006).
[28] Rotenberg Testimony, *supra* note 3, at 7.

ability to contact a specific individual, either physically or online, using one or more pieces of information collected from children online, such as user or screen names and/or passwords, zip code, date of birth, gender, persistent IP addresses, mobile geolocation information, information collected in connection with online behavioral advertising, or other emerging categories of information. Because operators are using such information to contact specific individuals, the definition of "personal information" in the Rule should be expanded to include such information.

In February of 2009, the FTC published a staff report promulgating voluntary guidelines for online tracking, monitoring, and advertising.[29] Then Commissioner John Leibowitz issued a separate, concurring statement[30] in which he questioned the non-mandatory nature of the guidelines:

> Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission. Put simply, this could be the last clear chance to show that self-regulation can—and will—effectively protect consumers' privacy in a dynamic online marketplace. . . .
>
> [A]lmost all of us want to see self-regulation succeed in the online arena, but the jury is still out about whether it alone will effectively balance companies' marketing and data collection practices with consumers' privacy interests. A day of reckoning may be fast approaching.[31]

The sensitivity of children's personal information establishes a clear case against self-regulation, and operators should not, therefore, be left to their own devices in policing their use of such information for advertising purposes.

f. Enumerated definitions for such terms as ''the physical or online contacting of a specific individual,'' ''website,'' ''online service,'' and other terms not currently defined should be added to § 312.2.

Each definition should be worded as expansively as possible so that operators are unable to avoid COPPA liability on semantic technicalities.

---

[29] U.S. FEDERAL TRADE COMMISSION, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; *see also* EPIC, *Trade Commission Issues Voluntary Guidelines for Online Tracking, Targeting, and Advertising*, http://epic.org/2009/02/trade-commission-issues-issue.html.

[30] U.S. FEDERAL TRADE COMMISSION, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, Concurring Statement of Commissioner Jon Leibowitz, (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.

[31] *Id.* at 1, 4.