



ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

“An Examination of Children’s Privacy:
New Technologies and the Children’s Online Privacy Protection Act (COPPA)”

Marc Rotenberg,
EPIC Executive Director

Before the

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, and Insurance

April 29, 2010
253 Russell Senate Office Building
Washington, DC

Introduction

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on “An Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection Act (COPPA)” My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC) and Adjunct Professor at Georgetown University Law Center.

EPIC is a non-partisan research organization, focused on emerging privacy and civil liberties issues. We have 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.”¹ We urged the FTC to investigate these business practices and to develop appropriate safeguards.

In 1996, I testified before the House Judiciary Committee in support of the bill that eventually became COPPA.² I warned: “The collection of data about children is growing at a phenomenal rate. Government agencies, private organizations, universities, associations, businesses, and club all gather information on kids of all ages. Records on our children are collected literally at the time of birth, segmented, compiled, and in some cases resold to anyone who wishes to buy them.”

EPIC worked with the Center for Media Education, which had published a groundbreaking study in 1996 on children’s privacy, to develop COPPA and help ensure 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. Targeting of children by marketing techniques resulted in the release of huge amounts of private information into the market and triggered the need for COPPA.³

¹ 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.

² Testimony and Statement for the Record of Marc Rotenberg, director Electronic Privacy Information Center on the Children's Privacy Protection and Parental Empowerment Act, H.R. 3508 Before the House of Representatives, Committee on the Judiciary, Subcommittee on Crime, September 12, 1996 *available at* http://www.epic.org/privacy/kids/EPIC_Testimony.html.

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>; *see also supra* notes 1-2.

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 new 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.⁴ 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.⁵ These emerging practices affect many consumers, but children are particularly vulnerable.

We appreciate your interest in children’s privacy and new technology, and we are grateful for the opportunity to appear before the Committee today.

The Purpose of COPPA and Structure of COPPA is Essentially Sound

The Children’s Online Privacy Protection Act, as set out in the FTC Rule, establishes a basic framework for privacy protection. COPPA requires any web site that collects personal information from children to: 1) “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;”⁶ 2) “obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;”⁷ 3) provide parents with access to the information collected from their children;⁸ and 4) “establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.”⁹

⁴ EPIC, *In re Facebook*, <http://epic.org/privacy/inrefacebook/>; EPIC, *In re Google Buzz*; <http://epic.org/privacy/ftc/googlebuzz/default.html>; EPIC, *Harris v. Blockbuster*, <http://epic.org/amicus/blockbuster/default.html>.

⁵ EPIC, *Privacy? Proposed Google/DoubleClick Merger*, <http://epic.org/privacy/ftc/google/>; EPIC, *Google Books Litigation*, <http://epic.org/privacy/googlebooks/litigation.html>.

⁶ 15 U.S.C. § 6502(b)(1)(A)(i) (2009).

⁷ 15 U.S.C. § 6502(b)(1)(A)(ii) (2009).

⁸ 15 U.S.C. § 6502(b)(1)(B) (2009).

⁹ 15 U.S.C. § 6502(b)(1)(D) (2009).

The FTC Rule that was promulgated included several innovative provisions, including one that prohibits 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 That provision wisely anticipated that web sites would try to extract data from children unless it was made clear that only the information necessary to provide the service should be obtained.

Some web sites,¹¹ including social network web sites,¹² comply with COPPA by implementing privacy safeguards for their young users. Many other web sites,¹³ including social network sites,¹⁴ allege that their sites do not collect personal information from children, and are therefore exempt from COPPA requirements. Disputes over COPPA typically focus on the age verification procedures and the scope of application.

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 as well as 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.

We supported COPPA at the time of enactment and continue to believe it provides a sound basis for privacy protection.

¹⁰ 15 U.S.C. § 6502(b)(1)(C) (2009).

¹¹ *E.g.* The Walt Disney Co., *Kids' Privacy Policy*, <http://corporate.disney.go.com/corporate/kids.html> ("Building on our general Privacy Policy, we recognize the need to provide additional privacy protections when children visit the sites on which this Kids' Privacy Policy is posted.").

¹² *E.g.* Yoursphere, *Yoursphere For Parents*, <http://internet-safety.yoursphere.com/news/twitter-facebook-coppa-the-yoursphere-difference> ("Yoursphere is a membership-based, online social community exclusively for youth through the age of 18. Here's how Yoursphere meets, and exceeds COPPA guidelines").

¹³ *E.g.* *N.Y. Times*, *The New York Times Privacy Policy Highlights*, ("The New York Times does not knowingly collect or store any personal information, even in aggregate, about children under the age of 13."); U.S. Bank, *Privacy Policy*, <https://loansandlines.usbank.com/loanslines/privacyPopup.do> ("We do not intentionally market to or solicit personal information from children under the age of 13.").

¹⁴ *E.g.* Facebook, *Help Center*, <http://www.facebook.com/help/?safety=parents> ("Facebook requires its users to be at least 13 years old before they can create an account. Providing false information to create an account is a violation of our Statement of Rights and Responsibilities.").

Social Networks Have Transformed Data Collection Practices

It is clear that the single biggest change impacting the privacy of children since the adoption of COPPA has been the emergence of social network services, such as Facebook, MySpace, and Twitter. These web-based platforms provide new opportunities for kids to interact online and also for companies to gather up information.

Leaving aside for the moment whether sites are currently in compliance with COPPA as they tend to discourage participation by those thirteen and under, I would like to focus on the broader implications that this technological change has had on children's privacy. In the simplest terms, COPPA did not anticipate the immersive online experience that a social network service would provide or the extensive data collection of both the trivial and the intimate information that children would share with these friends. This is not to say that the COPPA rules do not apply to all forms of data collection, rather the point is that the data collection and use is much more extensive than was anticipated.

We also see the increasingly opaque way that companies transfer user information to 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 not so easy for users to observe and control.

More specifically, 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.¹⁵ More recently, Senators Schumer, Bennet, Begich, and Franken have expressed to Facebook their concern about the most recent changes in Facebook's business model.¹⁶ Senator Schumer specifically asked the FTC to develop guidelines for these services.¹⁷ Similar concerns are likely to arise with Twitter as the company begins to incorporate advertising and to track the activities of its users.

¹⁵ EPIC, *In re Facebook*, <http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

¹⁶ Letter from Senator Charles Schumer, Senator Michael Bennet, Senator Mark Begich, and Senator Al Franken to Facebook CEO Mark Zuckerberg, Apr. 27, 2010 *available at* <http://voices.washingtonpost.com/posttech/Schumer-Franken-Bennet-Begich%20Letter%20to%20Facebook%204.27.10.pdf>.

¹⁷ *Id.*

There is a good argument that these data collection practices should be regulated for all users simply because all users have an interest in how their personal information is used by these firms. But the argument is particularly strong for teenagers, those between the ages of 13 and 18, who have no protection under COPPA and who cannot easily follow all of the changes taking place in this self-regulatory environment. In fact, in our recent complaint to the FTC concerning Facebook, we were struck by how many Internet commentators, bloggers, and security experts found it difficult to make sense of the recent changes in the Facebook privacy settings.¹⁸

Therefore, updates to COPPA should focus specifically on the collection and use of data in the social network world. Teenagers should be given much greater control over the collection of data about them.

The FTC Has Failed to Enforce Children’s Privacy Rights Despite Clear-Cut Violations

One of the growing concerns with COPPA is the failure of the Federal Trade Commission to vigorously enforce its provisions. Several years ago, there were notable enforcement actions by the FTC. For example, in September 2006, the FTC brought COPPA enforcement actions against several companies. The FTC fined the website Xanga \$1 million for failing to obtain parental consent for children under 13 even though the site clearly targeted this population.¹⁹ And the FTC fined UMG Recordings \$400,00 for similar violations.²⁰

But it is difficult to find news of any recent enforcement action. The FTC claims on its website:

The FTC has obtained numerous federal district court settlements against website operators who are alleged to have violated the COPPA Rule. Press releases, and the complaints and orders may be found at www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

¹⁸ *Supra* note 15 at 16-23.

¹⁹ 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>.

²⁰ FTC, *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/bonziung.shtm>.

But if you go to this link, you will find just one enforcement action over the last several years, which was taken against the Iconix Brand group and produced a fine of \$250,000.²¹

EPIC's experience with the recent Echometrix complaint is particularly telling. In September 29, 2009, EPIC filed a detailed complaint with the Federal Trade Commission alleging that Echometrix, a software company, was selling "parental control" software that was in fact monitoring children's online activity for marketing purposes.²² 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.²³

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

The Federal Trade Commission acknowledged receipt of the complaint, but never took an enforcement action against the company. As far as we know, they never even opened an investigation.

You might conclude that perhaps our complaint was mistaken or that maybe the company had changed its practices, but there is more to the Echometrix story. Not long after we filed the complaint with the FTC, we learned that the Department of Defense shared our concerns about this product, particularly as it would place at risk children in military families.

In an email that we obtained through a Freedom of Information Act request, we learned that the Manager of the AAFES' Exchange Online Mall, which provides products and services for military families around the world, wrote to Echometrix:

²¹ FTC, *Iconix Brand Group Settles Charges Its Apparel Web Sites Violated Children's Online Privacy Protection Act*, Oct. 20, 2009, <http://www.ftc.gov/opa/2009/10/iconix.shtm>.

²² EPIC, *In re Echometrix*, <http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf>; see EPIC, *EPIC-Echometrix*, <http://epic.org/privacy/echometrix/>

²³ 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=114428. The company has since changed its characterization of the Pulse service.

I was forwarded the attached complaint submitted to the FTC by EPIC. It is very unfortunate that you 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 your site, and it will stay offline until this matter with EPIC and the FTC is resolved.²⁴

The Department of Defense was able, with just a quick review of the privacy issues, to determine that this product should not be sold to military families. But the Federal Trade Commission, which has the statutory authority and presumably the expertise to investigate such matters, simply ignored it.²⁵

To this date, the FTC has not explained why it failed to take action.

Updates to COPPA

One area where there is a clear need to update COPPA concerns the scope of Personally Identifiable Information. Under the original rule, traditional categories of personal information, such as name, address, phone number and social security number are treated as "Personal information."²⁶ The Rule also wisely treats persistent identifiers, such as cookies, as personal information.²⁷ However, the Rule did not anticipate the emergence of the mobile web and location-based services. It is possible that such information could be considered as part of the catchall provision, section 312.2(g), but the better approach would be to make explicit that location information associated with an individual child should be included in the categories of personal information.

We would also recommend that serious consideration be given to raising the age of COPPA coverage. This was a hotly debated issue at the time of the law's enactment. At the time of introduction, the Children's Privacy Protection and Parental Empowerment Act of 1996, which later became COPPA, set the age

²⁴ 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.

²⁵ Jaikumar Vijayan, *DOD nixes vendor of online monitoring software over privacy concerns: EchoMetrix suspended from selling products via military's shopping portal*, Computerworld, Dec. 4, 2009, http://www.computerworld.com/s/article/9141821/DOD_nixes_vendor_of_online_monitoring_software_over_privacy_concerns.

²⁶ § 312.2 (Definitions).

²⁷ § 312.2(f).

requirement at 16. Eventually, to help ensure passage, the age requirement was dropped to 13. But it remains an opportunity, particularly now with the bill up for review, whether the privacy obligations should extend to those who are 16 or perhaps even 18.

Today, I recommend that Congress raise the age requirement in COPPA to 18. The emergence of social networks and the powerful commercial forces that are seeking to extract personal data on all users of these services, but particularly children, raise new challenges that the original COPPA simply did not contemplate. To the extent that companies choose to collect personal information on children between 13 and 18, they should be subject to privacy obligations. If they believe that the privacy obligations are too burdensome, the alternative is straightforward: provide an online experience that does not require the collection of so much personal data. Innovative companies, no doubt, will find clever new business models that respect users' privacy.

If the Congress chooses not to raise the age on COPPA, then I anticipate that the privacy problems will grow more severe in the next few years. Not only will companies that target young teens gather more data, their business practices will become increasingly more opaque and more difficult for users to manage. We have seen just in the last few years how companies such as Facebook have found that they can manipulate privacy settings and change privacy policies to coax personal information out of users who had earlier made clear which information they would reveal and which information they would keep private.

There is one proviso for this recommendation. For children in between the ages of 13 to 18, I believe that the companies subject to COPPA should have an obligation to provide privacy rights directly to the users of their services and not to their parents. By this I mean that it is the kids who should be able to learn how their personal data is being gathered and object where appropriate. I think this approach will encourage teenagers to exercise greater control over their online experience and to understand the privacy practices of the companies they deal with. While it is appropriate that parents make these decisions for younger children, creating privacy rights for teenagers is likely to lead to better informed decisions and greater consideration of privacy interests by companies providing online services.

The growing concerns about the FTC's ability to safeguard online privacy raises another concern and that is whether the FTC has the authority and the competence to address emerging privacy challenges. It is not just in the area of COPPA enforcement that there are concerns. The FTC has also shown an inability to address such important new topics as cloud computing, location privacy, or the broader question of the effectiveness of web privacy policies and self-regulation.

EPIC has had several important complaints pending at the FTC. Whereas previous Commissions acted forcefully on the recommendations of consumer privacy groups, the current FTC seems unwilling or unable to address the privacy challenges that confront users of new services every day.²⁸ In one particularly egregious example, it took the attack on Google in China in January of this year to get the company to routinely encrypt Gmail, something that EPIC had specifically recommended to the FTC in our March 2009 complaint.²⁹

There is another issue I would like to bring your attention to concerning children and new technology. While much of COPPA's focus is understandably directed toward the Internet and data gathering activity by commercial firms, it is important to consider also how new technologies are gathering data on children in public spaces and with new communications technologies. There is, for example, the use of RFID technology for identity documents that makes it possible to track and record the location of children. Properly implemented there may be some security benefits. But there are also substantial risks that should be considered. In one case, public objections led a school to drop its plan to require RFID-enabled tags for identity documents.³⁰

Conclusion

COPPA was a smart and forward-looking privacy law. It helped slow the commercialization of personal information concerning children and it promoted safety and respect for the treatment of minors using new online services. Around the edges, there are understandable questions about application and implementation. Age verification continues to be a challenge. But the central purpose – to establish privacy safeguards for the collection and use of personal information on children – is sensible and important. The critical task now is to carry forward this goal as new business practices continue to raise new privacy challenges.

Thank you for your interest. I will be pleased to answer your questions.

²⁸ Marc Rotenberg, "Does the FTC Care About Consumer Privacy?" 9 BNA Privacy and Security Law 453, 478 (March 29, 2010).

²⁹ EPIC, in re Google and Cloud Computing, <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf> at ¶¶9,30,47; see EPIC, *In re Google and Cloud Computing*, <http://epic.org/privacy/cloudcomputing/google/>.

³⁰ Wired, *School Drops RFID Tag Program*, Feb. 16, 2005, <http://www.wired.com/techbiz/media/news/2005/02/66626>.

REFERENCES

EPIC, "EPIC - Children's Online Privacy Protection Act (COPPA)"

<http://epic.org/privacy/kids/default.html>

EPIC, "EPIC – Cloud Computing"

<http://epic.org/privacy/cloudcomputing/>

EPIC, "EPIC – Echometrix"

<http://epic.org/privacy/echometrix/>

EPIC, "FTC Complaint on Amazon.com COPPA Compliance" (Apr. 22, 2003)

<http://epic.org/privacy/amazon/coppacomplaint.html>

EPIC, "Radio Frequency Identification (RFID) Systems"

<http://epic.org/privacy/rfid/>

EPIC, "In re Facebook"

<http://epic.org/privacy/inrefacebook/>

EPIC, "In re Google Buzz"

<http://epic.org/privacy/ftc/googlebuzz/default.html>

EPIC, "In re Google and Cloud Computing"

<http://epic.org/privacy/cloudcomputing/google/>

FTC, "Children's Online Privacy Protection Rule; Final Rule"

<http://www.ftc.gov/os/1999/10/64fr59888.htm>

FTC, "COPPA FAQs"

<http://www.ftc.gov/privacy/coppafaqs.shtm>

FTC, "How to Comply With The Children's Online Privacy Protection Rule"

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm>