AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 111–968

AN EXAMINATION OF CHILDREN'S PRIVACY: NEW TECHNOLOGIES AND THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

APRIL 29, 2010

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

66–284 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE McCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DeMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LeMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Republican Staff Director*
BRIAN M. HENDRICKS, *Republican General Counsel*
NICK ROSSI, *Republican Chief Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

MARK PRYOR, Arkansas, *Chairman*
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
CLAIRE McCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico

ROGER F. WICKER, Mississippi, *Ranking*
OLYMPIA J. SNOWE, Maine
JIM DeMINT, South Carolina
JOHN THUNE, South Dakota
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana

CONTENTS

	Page
Hearing held on April 24, 2010	1
Statement of Senator Pryor	1
Statement of Senator Wicker	2
Statement of Senator Rockefeller	3
Prepared statement	5
Statement of Senator Klobuchar	5

WITNESSES

Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission	7
Prepared statement	8
Timothy Sparapani, Director, Public Policy, Facebook	13
Prepared statement	14
Michael D. Hintze, Associate General Counsel, Microsoft Corporation	19
Prepared statement	21
Kathryn C. Montgomery, Ph.D., Professor, School of Communication, American University	33
Prepared statement	34
Marc Rotenberg, Executive Director, EPIC and Adjunct Professor, Georgetown University Law Center	40
Prepared statement	42
Berin Szoka, Senior Fellow and Director, Center for Internet Freedom, The Progress & Freedom Foundation	47
Prepared statement	49

APPENDIX

Response to written questions submitted by Hon. Mark Pryor to:	
Jessica Rich	99
Timothy Sparapani	102
Michael D. Hintze	104
Kathryn C. Montgomery	108
Berin Szoka	112

AN EXAMINATION OF CHILDREN'S PRIVACY: NEW TECHNOLOGIES AND THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

THURSDAY, APRIL 29, 2010

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:07 a.m. in room SR–253, Russell Senate Office Building, Hon. Mark Pryor, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. I'll go ahead and call our hearing to order this morning.

I want to welcome our witnesses, thank all of you all for being here.

This morning, we'll examine children's privacy and how well the Children's Online Privacy Protection Act, or COPPA, is working.

The Consumer Protection Subcommittee has jurisdiction over the Federal Trade Commission, which enforces this statute. The FTC is currently engaged in reexamining the implementation and effectiveness of COPPA. Protecting our children's online privacy and safety is a critical issue whose importance cannot be overstated. Online abuses, such as harassment, threats, and cyberbullying should never be tolerated.

Today's discussion could not come at a more pivotal time, as technology developments and innovations, while greatly beneficial in many respects, contribute to the complexity of today's online space.

I'm concerned about our kids' online safety, for a number of reasons:

First, we know that, while some companies are making great strides to protect young people from predators and online dangers, the disclosure of personal information by young people is prevalent. Researchers are still unpacking the implications of this disclosure.

Second, recent reports have suggested that location-based advertising is tied to social networking. It also appears that certain technologies, such as GPS tracking capabilities, could track children, without their knowledge. As more kids have access to phones, and as tracking devices and mobile technologies increase in sophistica-

tion, greater understanding of how children could be impacted is essential.

Third, we know that our young children are using the Internet now more than ever before, and we know that they represent a large portion of total online activity. And, according to one report, in the last 5 years, we have seen the time spent online by kids ages 2 to 11—ages 2 to 11—increase by 63 percent. Children of that age make up almost 10 percent of online users.

I'm interested in all the witnesses' thoughts regarding the appropriateness of the statute's age limits, what constitutes children's personal information, how parental consent is best achieved, and how operators maintain the confidentiality and security of the information that they do collect, when authorized, about children.

I know that this FTC is considering both how to better prevent the authorized collection or the use of children's information, and how to educate parents and teachers about the importance of encouraging children to protect themselves online.

And I look forward to hearing from all of our witnesses, especially FTC, on what they're doing. And I also want to thank all of our witnesses for being here today.

Not all members of the business community were willing to present their views. Specifically, we had asked Apple and Google to come, but they declined. I think that's unfortunate, because they are major players in this area. And we're going to have a long and in-depth conversation that starts today, but this is going to go on into the future, and I think it's unfortunate that Apple and Google chose not to participate in this discussion.

So, with that, I'd like to turn it over to my Ranking Member, Senator Wicker.

STATEMENT OF HON. ROGER F. WICKER, U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Thank you, Mr. Chairman, for holding this important hearing to examine the Children's Online Privacy Protection Act, COPPA, and its application in today's ever-changing technological world.

We, as the Subcommittee responsible for consumer protection, are mindful that protecting our children is essential, and I applaud you, Mr. Chairman, for your commitment toward this goal.

The Internet provides the opportunity to share information for both adults and children. This has led to our current revolution in the availability of information to almost anyone who has access to a computer.

A flood of information, however, brings new challenges. One such challenge has been how to ensure the privacy of information for children when they use the Internet.

COPPA was created to address the privacy concerns that arise with Internet users under the age of 13. This law has worked for many years to maintain the security of children's personal information when it is collected online. It also ensures that parents know what tools and resources are available to help them be more aware of, and have some control over, what their children are doing online.

I commend the FTC for its continued efforts to enhance parents' involvement in children's online activities. I particularly want to highlight the consumer education efforts at the FTC. Making consumers and businesses aware of their rights and responsibilities is one of the most effective ways to ensure that the law achieves its goals.

One of the best examples of this is the FTC's NetCetera guide, which teaches adults how to explain to children the risks that can be associated with online conduct. However, even with these efforts, there are still many challenges parents face in protecting their children's information online, and it is important that the law be equipped to meet those challenges as they develop.

Keeping pace with technological changes is a difficulty that many industries face. It seems that, almost every day, a new service, a new application, or a new product is unveiled that is a little faster, a little better, and a little more complicated than we were using yesterday. This presents new and unique challenges in efforts to make sure that technologies are safe for consumers.

I've been a parent for many years, and it is important to me to keep my children safe. I'm also a new grandparent, and I'm amazed to think about the opportunities that my 5-week-old granddaughter will have. Her generation will be able to access information and learn so much more than those of us in this room ever imagined. A significant portion of those opportunities will be available through online technology and innovations occurring today, tomorrow, and years into the future. These rapid and continued technological changes, however, can make it difficult to consider regulations for the Internet.

Our first priority is to ensure safety, but we must also take care not to stifle innovation and business development that drives our economy and makes possible so many of the opportunities available to our children.

There have been many suggestions about ways to improve COPPA and help it meet Congress's goals in today's world. However, there have also been many concerns expressed about the effect that these changes could have, not only on innovation, but also on the very goals that COPPA strives to achieve. I think it's important for us to take time to consider these conflicting concerns and better understand their ramifications in both children's online privacy and children's online experience.

Thank you, Mr. Chairman.

Senator Pryor. Thank you.

Senator Rockefeller?

STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. Thank you, Mr. Chairman.

And you've already pointed out the 60 million children who are availing themselves of these technologies, these days. And I listened to the good Senator from Mississippi, and I understand the need to encourage innovation. But, every time it's a choice between protecting children or protecting privacy and protecting innovation, we always seem to go with innovation, and we never go with privacy. So, that's what COPPA is all about.

And I'm shocked—I'm absolutely shocked that children from 2 to the age of 13—which is totally irrelevant, really; I mean, it ought to be "children"—"children are children up until 25," or something like that, aren't they? I mean, they're just——

[Laughter.]

The CHAIRMAN. It's ridiculous. So, they get YouTube, Google, Facebook, and then two somewhat less decent terms that no parent would want their child searching for on the web. And, of course, that's the point.

So, accessing these websites, whether they're well known or popular or outright illegal, have enormous privacy considerations. And this is not an innovation meeting; this is a privacy meeting. We do that in this committee; we protect people. And particularly, we protect children, because they are the most vulnerable of all.

So, a lot of these companies are collecting personal information, and that's a benign term, until it becomes very unbenign and people are giving up all kinds of information that—they have no idea.

So, we passed COPPA, as has been indicated. And the idea was to keep personal information private. But, then the whole world has changed since that happened, technologically. The entire world has changed. And so, the FTC began an important effort to review its rules. It actually probably should have done so—started somewhat earlier; and I want to talk about that, but at least they're doing it. And I really think that Congress has to take a very hard look at whether COPPA should be updated, if FTC isn't going to do it, to cover new kinds of information, new businesses.

And I look forward to working with Senator Pryor. And I want to echo what he said. I appreciate the fact that Microsoft and Facebook are here. I also do not appreciate the fact that Apple and Google are not here. And I'm curious as to why they're not. Was it too expensive to send an associate or legal counsel? Was it a financial matter; they couldn't get the people here because they couldn't afford the plane tickets? Were they trying to avoid something? Were they trying to hide something? When people don't show up when we ask—I have this power of the subpoena, which I would absolutely love to use. I have not, to this point. But, what it all does, it increases our interest in what they're doing and why they didn't show up. So, they made a stupid mistake by not showing up today, and I say, "Shame on them."

So, this is an introductory hearing. We're starting an important public discussion; all of us here, tremendously interested in this. And, you know, children's safety comes first, always.

And so, we begin. And, as the Chairman has said, this is going to be the first of a number of hearings. Children are to be taken seriously. They're not. They're part of an age that we're not part of in technology, and it's dangerous for them. There are all kinds of horrible things that they can see; parents don't know about it. They don't know about it, they don't know what the rules are. And so, we have responsibilities.

I thank the Chair.

[The prepared statement of Senator Rockefeller follows:]

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER IV,
U.S. SENATOR FROM WEST VIRGINIA

Thank you, Senator Pryor, for your outstanding work as Chairman of the Subcommittee on Consumer Protection.

According to a recent study, children ages 2 through 11 make up 9.5 percent of online users. That's nearly 16 million children, and the number is rapidly growing.

A decade ago, going online meant accessing the Internet on a computer in your home. Today, it also includes iPhones, portable games, and interactive TVs. As powerful and exciting as these new developments are, a changing world brings new risks.

For instance, a recent survey found that the top five Internet searches by children under 13 were for the terms: "YouTube," "Google," "Facebook," and two somewhat less decent terms that no parent would want their young child searching for on the web.

Accessing these websites, whether they are well-known and popular or outright illegal, have enormous privacy implications that I fear parents are unaware of, and I know children do not understand.

Many companies are collecting personal information and monetizing it. This commercial practice has a particular impact on our children.

We have a responsibility to understand this rapidly changing digital landscape and to give parents the tools they need to protect their children's privacy.

In 1988, we passed the Children's Online Privacy Protection Act, or "COPPA", requiring websites to get parents' consent before collecting or using any personal information from children.

Since then, the way children use the Internet has changed dramatically. Some online technologies that are nearly ubiquitous today did not even exist a few years ago.

So in January, the FTC began an important effort to review its rules. But with such rapid change, I firmly believe Congress also must take a hard look at whether COPPA should be updated to cover new kinds of information and new businesses. I look forward to working with Senator Pryor in this examination.

I very much want to thank Microsoft and Facebook for testifying. I have to say that I am disappointed Apple and Google have declined to participate today. These two companies are at the forefront of technological developments in the online world.

With this introductory hearing, we are starting an important public discussion with direct implications on children's privacy. Apple and Google's refusal to take part does not speak well of their commitment to working with Congress on this issue going forward.

I want to close by noting that children's *privacy* is strongly connected to children's *safety*, and I believe in my core that all children deserve special protections. Always. Period.

It's important not to conflate the two issues, but privacy and safety most certainly overlap.

To parents, nothing is more important than protecting our children. Nothing. I am enormously alarmed by the rise in criminal behavior targeting children online, from "cyber-bullying" to adult predators.

These frightening trends are directly connected to the fact that our children's sensitive, personal information is being increasingly exposed to the public.

I look forward to continuing this important discussion and working together—Congress, the FTC, and online stakeholders—to make sure nothing comes before the safety and security of our children.

Senator PRYOR. Thank you, Mr. Chairman.

And I would note for the record that Chairman Rockefeller has a long and distinguished and successful career in protecting children.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

And thank you, also, Senator Rockefeller, for all the work you've done in this area.

It's remarkable, as my colleagues have noted, how quickly technology has changed over the last few years. The old joke—I still remember this—people would say, "Well, if you want to program your VCR, ask your kid." But, now VCRs are a thing of the past. New technologies, devices, programs, and applications have completely changed the way we work and the way we communicate. From GPS and GeoLocation on Smartphones, to the ubiquity of text-messaging and Twitter, to posting our photos on social networking sites, the world is quickly changing.

And no group adapts to new technology quicker than young people. And as was noted by my colleagues, nearly 16 million kids aged 2 through 11 are active online, and they make up, I think, 9.5 percent of online users. And these numbers are growing as more and more young people are logging on. The average young child spends more than 11 hours a month on the Internet, a 63-percent increase over 5 years ago. And this is one of the more sad facts. One survey found that the top five Internet searches for children under 13 are YouTube, Google, Facebook, sex, and porn.

Clearly, the online world has changed dramatically. I think if you look back when these COPPA rules were adopted, 10 years ago, that wouldn't have been the case; you probably could have hardly even checked what kids were checking, and they probably weren't checking into any of these things. And so, it is very important that we examine this rule to ensure that it keeps up with the technology.

I've just heard a lot of stories in our state, working with Senator Thune on the peer-to-peer legislation that we have, of changing technology that while it's so great in so many ways for innovation, has also severely hurt people's privacy rights. And when it comes to kids, we reach a whole new level.

So, I'm looking forward to working with my colleagues to work on this rule and make changes that are in the best interest of everyone.

Thank you very much.

Senator PRYOR. Thank you, Senator Klobuchar.

And I would like to say that, for all of our witnesses—we have a very distinguished panel today, and that we could spend a lot of time introducing them and going through all their experiences and their degrees and all their backgrounds. And it's a very impressive group. But, that is all part of the record.

And so, what I'm going to do is, I'm just going to go down the line, introduce each one, and ask each one to make a 5-minute opening statement. And what I'd like for you all to do is just pay attention to the lights there in front of you, and when 5 minutes is over, we would love for you to, you know, wrap it up.

First, I would like to introduce Jessica Rich; she's the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission. Second is Timothy Sparapani, Director of Public Policy at Facebook. Next is Mike Hintze; he's the Associate General Counsel at Microsoft. Next is Kathryn Montgomery, Ph.D.; she's Professor of School of Communications at American University. Next is Marc Rotenberg; he's Executive Director of Electronic Privacy Information Center. And last, and certainly not least, at the children's table, here——

[Laughter.]

Senator PRYOR.—we have—and I'm sorry that our table is only so long this morning—but, anyway, we have Berin Szoka; he's Senior Fellow, Director of the Center for Internet Freedom at The Progress & Freedom Foundation.

So, thank all of you all for being here.

And, Ms. Rich, if you could lead us off.

STATEMENT OF JESSICA RICH, DEPUTY DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. RICH. Mr. Chairman and members of the Committee, I'm Jessica Rich, Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate this opportunity to update you regarding the FTC's work to protect children's privacy and enforce the Children's Online Privacy Protection Act, or COPPA.

We have submitted a written statement today which represents the views of the FTC. The views expressed orally, and my responses to questions, are my own and do not necessarily reflect the views of the Commission or any commissioner.

The Federal Trade Commission is deeply committed to helping to create a safer, more secure online experience for children. The Commission's rule implementing COPPA became effective 10 years ago. The statute and rule apply to operators of websites and online services directed to children under age 13 and to other website operators that have actual knowledge that they are collecting information from children.

Covered website operators must provide notice of their information collection practices and, with limited exception, obtain verifiable parental consent prior to the collection, use, or disclosure of personal information from children. Operators also must give parents the opportunity to review and delete personal information that their children have provided.

The Commission has taken a multipronged approach to rule compliance that includes enforcement, education, and implementation of the statutory mandated COPPA safe harbor program. On the enforcement side, the Commission has brought 14 law enforcement actions alleging COPPA violations. The FTC's early COPPA cases focused on children's sites that collected extensive amounts of personal information without providing notice to parents and obtaining their consent.

More recent enforcement actions have focused on operators of both general audience and child-directed social networking sites, and sites with interactive features that permit children to divulge their personal information online.

A crucial complement to our law enforcement efforts is educating businesses about their responsibilities under the law. The FTC has published comprehensive compliance materials, which are available on our website. We also devote significant resources to answering individual requests from companies about rule compliance, and to conducting outreach to industry groups. Our goal in these efforts is to prevent COPPA violations before they occur.

The Commission's consumer education materials aim to inform parents and children about the protections afforded by the rule, so

they know what to expect and what to look for as they navigate online. These materials are available through the Commission's online safety portal, *OnGuardOnline.gov*. OnGuardOnline provides practical and plain-language information about COPPA and other privacy and safety topics, in a variety of formats, including articles, games, quizzes, and videos.

Our most recent addition is the NetCetera guide, which Senator Wicker was kind enough to mention at the beginning.

In light of significant changes to the online environment, including the explosive growth of social networking, mobile web technologies, and interactive gaming, the Commission recently initiated a review of the rule.

On March 24 of this year, the Commission launched a public comment period aimed at gathering input on a wide range of issues, including whether the rule's definition of "Internet" adequately covers certain types of mobile communications and interactive media, whether the rule's definition of "personal information" has kept pace with technological developments—that is, whether certain information that isn't named and listed in the rule, such as static IP address, could allow a website to contact a child; the effectiveness of mechanisms used to—and another topic is the effectiveness of mechanisms used authenticate parents who provide consent or seek access to their children's information.

The comment period for these questions closes on June 30. On June 2, the Commission will host a public roundtable, here in Washington, to hear from stakeholders, including children's privacy advocates, website operators, businesses, academics, educators, parents, anyone who would like to come, on these important issues.

The Commission takes seriously the challenge to ensure that COPPA continues to meet its originally stated goal, even as children's interactive media use moves from standalone PCs to other devices.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Rich follows:]

PREPARED STATEMENT OF JESSICA RICH, DEPUTY DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

I. Introduction

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, my name is Jessica Rich, and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("Commission").[1] I appreciate the opportunity to appear before you today to discuss the Commission's implementation of the Children's Online Privacy Protection Act of 1998 ("COPPA").[2]

The Federal Trade Commission is deeply committed to helping to create a safer, more secure, online experience for children. As such, the agency has actively engaged in law enforcement, consumer and business education, and rulemaking initiatives to ensure that knowledge of, and adherence to, COPPA is widespread. In the past 10 years, the Commission has brought fourteen law enforcement actions alleging COPPA violations and has collected more than $3.2 million in civil penalties. In addition, in light of significant changes to the online environment, including the explosion of social networking and the proliferation of mobile web technologies and

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6508 (2009). The Commission's implementing regulations (the "COPPA Rule") are found at 16 C.F.R. Part 312 (2009).

interactive gaming, and the possibility of interactive television, the Commission has recently initiated an accelerated review of COPPA's effectiveness.

This testimony first provides a brief legislative and regulatory overview of COPPA. It next summarizes the Commission's efforts to enforce COPPA and to educate businesses and consumers about the law. Finally, it discusses the Commission's current initiative to review its COPPA Rule in order to determine whether the Rule should be modified to address changes in technology that may affect children's privacy.

II. A Brief COPPA Overview

A. The Legislation

Congress enacted COPPA in 1998 to address the unique privacy and safety risks created when young children—those under 13 years of age—access the Internet. COPPA's legislative history reveals several critical goals: (1) to enhance parental involvement in children's online activities in order to protect children's privacy; (2) to protect children's safety when they visit and post information on public chat rooms and message boards; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent.[3]

COPPA applies to operators of websites and online services directed to children under age 13, and to other website operators that have actual knowledge that they are collecting personal information[4] from such children (collectively, "operators"). The statute generally mandates that operators covered by the Act provide notice of their information collection practices and, with only limited exceptions, obtain verifiable parental consent *prior* to the collection, use, or disclosure of personal information from children. Operators also must give parents the opportunity to review and delete personal information their children have provided. Operators are required to establish and maintain reasonable procedures to protect the security of personal information collected from children, and must not condition children's participation in website activities on the disclosure of more personal information than is reasonably necessary.[5]

COPPA contains a safe harbor provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines to implement the statute's protections.[6] The statute provides that operators who fully comply with an approved safe harbor program will be "deemed to be in compliance" with the Commission's COPPA Rule for purposes of enforcement.[7]

B. The Commission's COPPA Rule

COPPA mandated that the Commission promulgate and enforce regulations to implement the Act. The Commission published for public comment a proposed Rule in April 1999, and in November 1999 published its final Rule, which went into effect on April 21, 2000.[8]

The Rule closely follows the statutory language, requiring operators to provide notice of their information practices to parents and, with limited exceptions, to obtain "verifiable parental consent" prior to collecting, using, or disclosing personal information from children under the age of 13. Verifiable parental consent, as set forth in the Rule, means that operators must use a consent method that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.[9] The COPPA Rule sets forth a sliding scale approach to obtaining verifiable parental consent based upon the risks posed by the intended

---

[3] *See* 144 Cong. Rec. S12741 (Oct. 7, 1998) (statement of Sen. Bryan).

[4] COPPA defines personal information as individually identifiable information about an individual collected online, including: a first and last name; a home or other physical address including street name and a name of a city or town; an e-mail address; a telephone number; a Social Security number; any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or 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. 15 U.S.C. § 6501(8).

[5] 15 U.S.C. § 6503(b)(1).

[6] 15 U.S.C. § 6504. Since the Commission's COPPA Rule took effect on April 21, 2000, four groups have received Commission approval of their safe harbor programs: the Children's Advertising Review Unit of the National Advertising Division of the Council of Better Business Bureaus ("CARU"), the Entertainment Software Rating Board ("ESRB"), TRUSTe, and Privo, Inc. For information on the Commission's COPPA safe harbor process, *see http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html*.

[7] 15 U.S.C. § 6504(b)(2).

[8] 16 C.F.R. § 312 (2009).

[9] 16 C.F.R. § 312.5(b)(1).

uses of the child's information.[10] Under this approach, operators who keep children's information internal, and do not disclose it publicly or to third parties, may obtain parental consent by methods such as sending an e-mail to the parent and then following up to confirm consent.[11] By contrast, operators who disclose children's personal information to others must use a more reliable method of parental consent—either one of the methods outlined by the Commission, or an equivalent method designed to ensure that the operator is connecting with the child's parent.[12]

COPPA authorizes the Commission to enforce the Rule in the same manner as it does rules promulgated under Section 18(a)(1)(B) of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices.[13] This permits the Commission to obtain civil penalties against operators who violate the Rule. COPPA further authorizes state attorneys general to enforce compliance with the Rule by filing actions in Federal court with written notice to the Commission.[14]

III. The Commission's COPPA Enforcement and Education Efforts

A. Enforcing COPPA

In the 10-years since the Rule's enactment, the Commission has brought fourteen (14) COPPA enforcement actions that cut to the core of COPPA's goals—ensuring that parents are informed and have the right to say "no" before their young children divulge their personal information. These rights are especially important when, with the mere click of a mouse or the touch of a screen, a child's personal information can be viewed by anyone. Together, the Commission's actions have garnered more than $3.2 million in civil penalties.[15]

In 2006, as social networking exploded onto the youth scene, the Commission redoubled its efforts to enforce COPPA. That year, the Commission obtained an order against *Xanga.com,* a then-popular social blogging site alleged to have knowingly collected personal information from, and created blog pages for, 1.7 million underage users—without obtaining their parents' permission. The *Xanga.com* settlement included a $1 million civil penalty.[16]

In 2008, the Commission obtained orders against two other operators of social networking sites. In January of that year, operators of the child-directed social networking site, *Imbee.com,* paid $130,000 to settle charges that they allegedly violated COPPA by collecting and maintaining personal information from over 10,500 children without first obtaining parental consent.[17] Later that year, Sony BMG Music Entertainment paid a $1 million civil penalty to resolve allegations that the company knowingly and improperly collected a broad range of personal information from at least 30,000 underage children who registered on 196 of its general audience music fan sites.[18]

Most recently, the Commission charged Iconix Brand Group, Inc., the owner and marketer of several apparel brands popular with children and teens, with collecting and storing personal information from approximately 1,000 children without first notifying their parents or obtaining parental consent. The Commission's complaint further alleged that on one of its brand websites, Iconix enabled girls to share per-

---

[10] 16 C.F.R. § 312.5(b)(2).

[11] The sliding scale mechanism, which initially was designed to expire in April 2002, was subsequently extended by the Commission. In 2006, the Commission announced that it would extend the sliding scale approach indefinitely. *See* 71 Fed. Reg. 13247 (Mar. 15, 2006), available at *www.ftc.gov/os/2006/03/P054505COPPARuleRetention.pdf.*

[12] Such methods include, but are not limited to: using a print-and-send form that can be faxed or mailed back to the operator; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the above methods. 16 C.F.R. § 312.5(b)(2).

[13] 15 U.S.C. §§ 6503(c), 6506(a), (d); 15 U.S.C. § 57a(a)(1)(B) (2009).

[14] 15 U.S.C. § 6505. To date, only the state of Texas has filed law enforcement actions under the COPPA statute. *See* News Release, Office of Texas Attorney General Abbott Takes Action Against Web Sites That Illegally Collect Personal Information from Minors: Millions of Children Registered With The Popular Sites; Texas first state to take action under COPPA (Dec. 5, 2007), *http://www.oag.state.tx.us/oagNews/release.php?id=2288.*

[15] News releases detailing each of the Commission's COPPA cases are available at *www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.*

[16] *United States* v. *Xanga.com, Inc.*, No. 06–CIV–6853(SHS) (S.D.N.Y.) (final order Sept. 11, 2006).

[17] *United States* v. *Industrious Kid, Inc.*, No. 08–CV–0639 (N.D. Cal.) (filed Jan. 29, 2008).

[18] *United States* v. *Sony BMG Music Entm't*, No. 08–CV–10730 (S.D.N.Y.) (final order Dec. 15, 2008).

sonal stories and photos publicly online. Iconix agreed to pay a $250,000 civil penalty to settle the Commission's charges.[19]

B. Consumer and Business Education

Although law enforcement is a critical part of the Commission's COPPA program, enforcement alone cannot accomplish all of the agency's goals in administering COPPA and the Rule. A crucial complement to the Commission's formal law enforcement efforts, therefore, is educating consumers and businesses about their rights and responsibilities under the law. By promoting business and consumer education, the Commission seeks to help the greater online community create a culture that protects children's privacy and security.

The Commission's business outreach goals focus broadly on shaping prospective practices. The agency devotes significant resources to assisting website operators with Rule compliance, regularly updating business education materials and responding to inquiries from operators and their counsel.[20]

The Commission's consumer education materials aim to inform parents and children about the protections afforded by the Rule and also provide them with general online privacy and safety information. The Commission's consumer online safety portal, OnGuardOnline.gov, provides practical and plain language information in a variety of formats—including articles, games, quizzes, and videos—to help computer users guard against Internet fraud, secure their computers, and protect their personal information.[21] The Commission's booklet, *Net Cetera: Chatting With Kids About Being Online*, is a recent addition to *OnGuardOnline.gov*. This guide gives practical tips on how parents, teachers, and other trusted adults can help children reduce the risks of inappropriate conduct, contact, and content that come with living life online. Net Cetera focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy.[22] The Commission has partnered with schools, community groups, and local law enforcement to publicize Net Cetera, and has distributed more than 2.5 million copies of the guide since it was introduced in October 2009.

IV. The Current Regulatory Review

In 2005, the Commission commenced a statutorily required review of its experience in enforcing COPPA.[23] Specifically, Congress directed the Commission to evaluate: (1) operators' practices as they relate to the collection, use, and disclosure of children's information, (2) children's ability to obtain access to the online information of their choice; and (3) the availability of websites directed to children. At the same time, the Commission sought public comment on the costs and benefits of the Rule, including whether any modifications to the Rule were needed in light of changes in technology or in the marketplace.

After completing that review, in 2007 the Commission reported to Congress that, in keeping with the legislative intent, the Rule: (1) played a role in improving operators' information collection practices and providing children with greater online protections than in the era prior to its implementation; (2) provided parents with a set of effective tools for becoming involved in and overseeing their children's interactions online; and (3) did not overly burden operators' abilities to provide interactive online content for children. Accordingly, the Commission concluded that there was a continuing need for those protections, and that the Rule should be retained

---

[19] *United States* v. *Iconix Brand Group, Inc.*, No. 09–CV–8864 (S.D.N.Y.) (final order Nov. 5, 2009).

[20] To facilitate COPPA compliance, the Commission maintains a comprehensive children's privacy area on its website where businesses can find useful publications, including *How to Comply with the Children's Online Privacy Protection Rule; You, Your Privacy Policy and COPPA*; and *How to Protect Kids' Privacy Online*, as well as answers to Frequently Asked Questions (or "FAQs"). *See http://www.ftc.gov/privacy/privacyinitiatives/childrens.html*. Periodically, the Commission issues guidance on specific topics, like the Rule's requirements for the content of online privacy notices, and the COPPA "actual knowledge" standard for operators of general audience websites. In addition, the agency maintains a COPPA Hotline, where staff members offer fact-specific guidance in response to questions from website operators.

[21] The OnGuardOnline.gov website is the central component of the OnGuardOnline consumer education campaign, a partnership of the Federal Government and the technology community. Currently, 13 Federal agencies and a large number of safety organizations are partners on the website, contributing content and helping to promote and disseminate consistent messages.

[22] *See* OnGuardOnline, "Net Cetera: Chatting With Kids About Being Online," available at *http://www.onguardonline.gov/pdf/tec04.pdf*.

[23] *See* 15 U.S.C. § 6506(1).

without change.[24] At that time, the Commission also acknowledged that children's growing embrace of mobile Internet technology and interactive general audience sites, including social networking sites, without the concomitant development of suitable age-verification technologies, presented challenges for COPPA compliance and enforcement.[25]

Although the Commission generally reviews its rules approximately every 10 years, the continued rapid-fire pace of technological change, including an explosion in children's use of mobile devices and participation in interactive gaming, and the possibility of interactive television, led the agency to accelerate its COPPA review by 5 years, to this year.[26] Accordingly, on March 24, 2010, the Commission announced the start of a public comment period aimed at gathering input on a wide range of issues relating to the COPPA Rule, including:

- The implications for COPPA enforcement raised by mobile communications, interactive television, interactive gaming, and other similar interactive media and whether the Rule's definition of "Internet" adequately encompasses these technologies;
- Whether operators have the ability, using persistent IP addresses, mobile geolocation data, or information collected from children online in connection with behavioral advertising, to contact specific individuals, and whether the Rule's definition of "personal information" should be expanded accordingly;
- How the use of centralized authentication methods (such as OpenId) will affect individual websites' COPPA compliance efforts;[27]
- Whether there are additional technological methods to obtain verifiable parental consent that should be added to the COPPA Rule, and whether any of the methods currently included should be removed; and
- Whether parents are exercising their rights under the Rule to review or delete personal information collected from their children, and what challenges operators face in authenticating parents.[28]

The period for comment on these questions will close on June 30, 2010. On June 2, before the comment period closes, the Commission will host a public roundtable at its Washington, DC Conference Center to hear from stakeholders—children's privacy advocates, website operators, businesses, academics, and educators and parents—on these important issues.[29]

V. Conclusion

The Commission takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals, even as children's interactive media use moves from stand-alone PCs, to handheld devices, and potentially beyond.

Thank you for this opportunity to discuss the Commission's COPPA program. I look forward to your questions.

Senator PRYOR. Thank you.
Mr. Sparapani?

---

[24] *See* Fed. Trade Comm'n, Implementing the Children's Online Privacy Protection Act: A Report to Congress (2007), available at *http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf*.

[25] *See id.* at 28–29.

[26] The Commission recently concluded a series of privacy roundtables exploring the challenges posed by the array of new technologies that collect and use consumer data. The Commission also sought public comment on these issues and currently is examining the comments and information developed at the roundtables. In addition, the Commission expects that information gathered during the course of the COPPA Rule review will help inform this broader privacy initiative. See Exploring Privacy: A Roundtable Series, *http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml*.

[27] Centralized authentication methods offer a means for users to log on to different services using one digital identity. Services such as OpenId replace the common login process on individual websites with a single authenticated identification to gain access to multiple software systems. As a result, children who obtain an OpenId authentication might be able to gain backdoor access to websites that otherwise would have provided them with COPPA protections or prevented their entry.

[28] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 75 Fed. Reg. 17089–93 (Apr. 5, 2010); see also News Release, Fed. Trade Comm'n, "FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule" (Mar. 24, 2010), *http://www.ftc.gov/opa/2010/03/coppa.shtm*.

[29] *See* News Release, Fed. Trade Comm'n, "Protecting Kids' Privacy Online: Reviewing the COPPA Rule" (Apr. 19, 2010), *http://www.ftc.gov/opa/2010/04/coppa.shtm*.

STATEMENT OF TIMOTHY SPARAPANI, DIRECTOR, PUBLIC POLICY, FACEBOOK

Mr. SPARAPANI. Chairman Pryor and Rockefeller, Ranking Member Wicker, and other Subcommittee members, thank you for your leadership and for inviting me to share Facebook's perspective on child safety, and how Facebook's innovations promote a safer online environment for teens.

From our inception, Facebook sought to provide a safer environment for all its users than was generally available on the Web. Facebook is not directed at children less than 13 years of age residing in the U.S., and does not knowingly collect information from any children under 13 in the U.S. Nevertheless, we take seriously our responsibilities to protect children under 13 and enhance teen users' online safety.

Accordingly, Facebook was built with COPPA's requirements in mind. Our commitment to keeping children off the site starts by requiring those trying to establish an account to enter their age on the very first screen. This birth date field prohibits children under 13 from establishing an account. This age-gate technology places a persistent cookie on the device used to attempt to establish an underage account, preventing the user from attempting to modify their birth date. When Facebook becomes aware of accounts established by children under 13, we terminate those accounts and delete all information.

We emphasize two points today. First, Facebook's real-name culture and innovative technologies and policies enhance online safety and privacy for teens. And, two, Congress should not overhaul COPPA, but, rather, support and encourage, not discourage or prohibit, companies' innovations to advance child and teen online safety, security, and privacy.

Facebook's approach to providing online safety leadership begins with the recognition that no existing system today can verify age of users online. As a result, Facebook developed an innovative, multilayer system to act as technological proxies for age verification. These layers are enhanced by Facebook's real-name culture, which helps us identify fake accounts.

Before Facebook, Internet users were warned to avoid sharing their real names and information online. Facebook was the first major Internet site that required people to build their profiles and networks using real names. This made Facebook less attractive to predators and other bad actors, who prefer not to use their real names and identities. People are also less likely to engage in negative, dangerous, or criminal behavior when their friends can see their name, their speech, and their information that they're sharing. This real-name culture, therefore, creates accountability and deters bad behavior.

Since Facebook users understand that their actions are recorded digitally, when users violate our site rules or the law, we can pinpoint corrective action to the specific account involved.

Our real-name culture also empowers users to become community police and report violations. Facebook's users click our report button, found throughout the service, when they see inappropriate behavior. This substantially multiplies the number of people re-

viewing content and behavior, which we think greatly enhances teen safety.

Further, Facebook's innovative privacy tools allow users to exercise direct control and share what they want with whom they want and when they want. This empowers users of all ages to protect themselves online. If a user feels uncomfortable connecting with a particular person, she may decline that friend request. If a user feels that a friend is annoying, harassing, or dangerous, she may block or de-friend that person, which terminates the user's connection and prevents further contact.

Further, Facebook's proprietary technologies allow us to continuously improve online safety and combat emerging online threats. Although we do not generally discuss these matters publicly, for fear that they may be circumvented or compromised, these technologies allow Facebook to perform ongoing authentication checks. We look for behavior that does not fit the patterns created by the aggregate data from our 400 million users. Let me tell you that suspicious behavior does stand out, which initiates a Facebook inquiry and immediate remedial actions.

Facebook employs additional age-gating technologies to limit the contact and sharing between minors and adults; thus, reducing the opportunities for adults to pose as minors.

Additionally, while those over 18 on Facebook can share information with everyone, Facebook automatically limits minor sharing to a much smaller subset of users, such as the minor's friends, friends of friends, and those in their verified networks, typically in their schools. This substantially reduces the visibility of minors to non-minors whom they do not know.

Further, Facebook recognizes the importance of collaborating with others to innovate in this area. We're proud of our relationships with child and safety security experts and with law enforcement. We are particularly proud of our relationships with the attorneys general.

In conclusion, although Facebook is not a service that is directed at children under 13, we've built our service, policies, and tools with COPPA in mind. Our experience tells us that Congress need not amend COPPA, at this time. In fact, any amendments might undo many of our innovative privacy and safety tools. Congress can, however, assist companies like us in advancing online child and teen safety by eliminating disincentives for child safety innovation. Congress should ensure regulators are not discouraging technological and policy safety advances when reviewing privacy and security policies and technologies at companies, like ours, that are trying to do the right thing.

Thank you.

[The prepared statement of Mr. Sparapani follows:]

PREPARED STATEMENT OF TIMOTHY SPARAPANI, DIRECTOR, PUBLIC POLICY, FACEBOOK

Thank you Chairman Pryor, Ranking Member Wicker and Subcommittee Members. My name is Tim Sparapani and I am Director, Public Policy for Facebook. Thank you for inviting me to testify today concerning Facebook's perspective on online child safety. We are pleased to discuss some of our innovations that lead to a safer online environment. We believe these innovations—some of which are obvious

to users and others that are not—are a key to providing a positive online experience.

Facebook started in 2004 as a social networking site for college and university students and from inception, Facebook sought to provide a safer environment for all its users than was generally available on the web. Although Facebook is not directed to young children—you must be 13 years of age or older to join Facebook—the Company takes special steps to insure that users under 18 have a safer experience.[1]

Facebook has been involved with many online safety initiatives around the world, such as the U.S. State Attorneys General Internet Technical Task Force, the UK Home Office Task Force on Child Safety, the EU Safer Internet initiative, the Australia Attorney General's Online Safety Working Group and others. Today, I would like to discuss the important ways that Facebook innovation helps promote a safer online environment. We also encourage Congress to encourage, not discourage or prohibit, companies' innovation in policies and technologies to promote child online safety, security and privacy. We believe that our innovations in teen online safety, security and privacy advance the cause of online safety for children.

Summary of Key Points and Request for Congressional Action

We wish to emphasize four points today and enlist Congress' assistance to advance child online safety.

- *Facebook's real name culture and innovative technologies and policies enhance online safety and privacy for teens.*
- *Facebook expends extensive effort on key teen safety issues that further reduce teen risks.*
- *Facebook collaborates with experts, law enforcement, and government agencies to develop a safer Internet.*
- *Congress has a role to play to support and encourage, not discourage or prohibit companies' innovations to advance child and teen online safety, security and privacy.*

We request, therefore, that Congress not overhaul COPPA, but instead provide legislative and regulatory incentives to companies to innovate on child safety and privacy technologies, and prevent regulators from foreclosing innovation and experimentation in this area.

Our testimony lays out in brief a number of the key innovations employed by Facebook to promote safety for teens and others online.

Facebook Innovation 1: A Real Name Culture Promotes Online Safety

Facebook's approach to providing online safety leadership begins with the recognition that there is no existing system today that can verify the age of a child online. As a result, Facebook developed and implemented an innovative, multi-layer system to act as technological proxies for age. These layers are discussed in greater detail below and are enhanced by Facebook's innovation of using a "real name" culture, which allows us to better filter out fake accounts and identify inappropriate contact.

Before Facebook, the common wisdom was that Internet users should avoid using their real names and sharing information online. Facebook was the first major web service that required people to build their profiles and networks using real names, and provided them with privacy tools to enable them to decide who could access that information. This important policy and technical architecture decision not only allowed Facebook users to become more connected, but also made the site safer. A culture of authentic identity made Facebook less attractive to predators and other bad actors who generally do not like to use their real names or e-mail addresses.

Facebook's real name culture also attracts users who are more likely to adhere to our Statement of Rights and Responsibilities (SRR, or what other companies call Terms of Service) and keep their behavior consistent with the standards of their communities. People are less likely to engage in negative, dangerous or criminal behavior online when their friends can see their name, their speech and the information they share. The real name culture creates accountability and deters bad behav-

[1] Facebook is not directed at children less than 13 years of age residing in the United States and does not knowingly collect information from any children under 13 in the United States. Nevertheless we recognize and take seriously our responsibilities as a corporation to protect children and enhance the online safety of children 13 years of age and older who are our users. Accordingly, Facebook was built with the requirements of the Child Online Privacy Protection Act (COPPA) in mind. When Facebook becomes aware of accounts established by children under the age of 13 we terminate those accounts and delete all the information uploaded by that account.

ior since Facebook users understand that their actions on our service create a record of their behavior. When users actions violate our SRR or the law, we can pinpoint corrective action—usually account termination and/or referral to law enforcement in potential criminal matters—to the specific account involved. Similarly Facebook is often able to detect fakes because of the types of connections made by a fake user account. And, of course, it's difficult to connect to friends using a fake account, since they are more likely to reject friend requests from people they do not know. Facebook also routinely blocks the registration of accounts under common fake names.

Our real name culture also empowers users to become "community policemen," and report those whose behavior violates Facebook's SRR. Facebook's users regularly use our report button, found throughout the service. This substantially multiplies the number of people reviewing content and behavior on Facebook and greatly enhances safety of teens on Facebook. At the same time, user actions often appear in the newsfeeds of his or her friends. If a friend learns of inappropriate behavior, he or she can intervene with a user to determine whether something is wrong.

Facebook Innovation 2: User Control on Facebook Enhances Privacy and Safety

Since its inception, Facebook has built innovative privacy tools for users to exercise direct control and share what they want, with whom they want, and when they want. This user control model supplements the protections designed into our service and empowers our users of all ages to protect themselves online.

Perhaps more importantly for this hearing, Facebook's user control model also allows users to determine whom they are connected with on Facebook. Facebook users must accept a request from another user to be connected—Facebook never makes that choice. If a user feels uncomfortable connecting with a particular person, she may decline that friend request. Further, if a user begins to feel that a friend on Facebook is annoying, spamming, harassing, and/or dangerous, she may de-friend that person at any time. This action of de-friending terminates the connection between the users and prevents further contact.[2] A user may also "block" another user in order to prevent any contact between the two. And, any user may at any time use our ubiquitous report button to draw Facebook's attention to inappropriate behavior.

Facebook takes its commitment to innovating to advance user privacy seriously. When new users sign up, they are introduced to our privacy help center, which explains how they may set a privacy setting for each piece of content the user shares. In December 2009, we introduced an unprecedented privacy dialog, which required every Facebook user, worldwide, to stop and consider their privacy settings before they could use the service further. As a result of that process, an additional one-third of our users customized their privacy settings.

Facebook Innovation 3: Hidden Security Systems and Safety Tools Advance Facebook Users Online Safety

Facebook's safety innovations extend to the development and use of proprietary technologies that allow us to continuously improve online safety and combat emerging online threats. Although we do not generally discuss these publicly for fear that they maybe compromised or circumvented, these technologies allow Facebook to perform ongoing authentication checks, including technical and community verifications of users' accounts. We look for anomalous behavior in the aggregate data produced by our 400 million users. For example, if an adult sends an unusual number of friend requests to unrelated minors which are ignored or rejected, our systems could be triggered, sending up a red flag and initiating a Facebook inquiry and remedial actions.

Facebook Innovation 4: Facebook Employs Age Gates to Limit Sharing and Connections Between Minors and Adults

As stated earlier, Facebook is neither directed at children less than 13 years of age nor does Facebook knowingly collect information of those under 13. Our privacy policy is explicit in this regard:

> If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that

[2] It should be noted that the de-friending and blocking occurs without notification, so the connection is simply, elegantly, electronically severed without drawing attention to the ending of the connection.

information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this help page.

Accordingly, Facebook is not required to comply with many of COPPA's requirements. However, Facebook actively removes accounts once discovered, of anyone it learns is under 13. It also employs a number of age gating technologies to limit the contact, sharing and connections between minors and adults. Facebook limits minors' access to the service by requiring those entering *Facebook.com* to type in their age on the very first screen.[3] This birth date field prohibits children under the age of 13 from establishing an account. The age gate technology places a persistent cookie on the device used to establish an account, preventing the user from attempting to modify their birth date.

Facebook further employs a separate set of age restrictions to further limit contact between minors and adults. These restrictions are intended to limit opportunities for adults to pose as minors. Facebook engages in what we call social verification to ask minors that are new to our service to consider the source of a new friend request. Along with the friend request we may interpose a question to the minor prior to the minor being able to confirm that they wish to accept that request. Typical representative questions asked of the minor: (i) Is this someone whom you know from your school?; or (ii) Is this someone whom you or your parents know from your community? We also limit the number of friend requests that anyone can send in a set period of time to further reduce unwanted contacts between unrelated users.

Additional limitations further limit the sharing of data between minors and adults on Facebook. While those over 18 on Facebook can share information with everyone, Facebook automatically restricts users under 18 from doing so. Facebook automatically limits their sharing to a much smaller subset of users, such as the minor's friends, friends of those friends, and their verified networks, generally associated with their schools. This limitation substantially reduces the visibility of minors to non-minors whom they do not know.

Face Book Innovation 5: Facebook Engages in Extensive Additional Safety Efforts to Combat Specific Threats to Teens Online

Facebook innovations also combat specific threats to teens on our service and the company cooperates closely with law enforcement on these issues, upon receipt of appropriate legal process.

Suicide and Self-Harm

Facebook regularly delivers information to each user's networks of friends. As a result, Facebook stands in a special position to help reduce teen suicides and other forms of self-harm. Users who witness changes in their friends' behavior, reflected in their Facebook postings, can intervene to prevent friends from harming themselves. The promotion of self-harm, including eating disorders, cutting, etc., is a violation of Facebook's Statement of Rights and Responsibilities, and we encourage users to report this information. Our dedicated team of User Operations analysts reviews these reports and removes content such as photos, groups, and events. When we receive a report of someone who has posted suicidal content on Facebook, we alert the National Suicide Prevention Lifeline and encourage the user to contact his or her local authorities/law enforcement immediately. We've also posted an FAQ to the privacy and safety page in our Help Center with information and links to suicide help resources. Facebook saves lives on a regular basis by helping to prevent this kind of behavior. Our real name culture helps people identify those who are truly in need and respond in real time to a cry for help.

Cyberbullying and Harassment of Teens Online

Facebook has led efforts around the world to help combat cyberbullying. In the U.S., Facebook was a founding member of the Stop Cyberbullying Coalition. Our robust reporting infrastructure leverages Facebook's 400 million users to monitor and report offensive or potentially dangerous content. This infrastructure includes, systems to prioritize the most serious reports, and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed. The team treats reports of harassing messages as a priority, reviewing and acting on most within 24 hours. We also prioritize serious reports submitted through the contact forms in our Safety Center. With assistance from our outside experts on our Safety Advisory Board we have produced new materials on our Safety Center that specifically address how to prevent or respond to cyberbullying. We have also partnered with

[3] The Subcommittee should note that many other leading online companies and social networks never even attempt to collect users' date of birth, and, therefore, never even attempt to block minors from using their sites and services.

other organizations like MTV on their "A Thin Line" campaign to educate young people about the dangers of digital abuse; with the BBC on their "bullyproof" campaign, and regularly invite experts, such as the National Crime Prevention Council to address cyberbullying on the Facebook Blog, which reaches over 8 million people.

Missing Children and Runaways

Facebook has also been successful in helping to locate missing teens. Law enforcement has generously praised Facebook for prioritizing law enforcement requests for IP location information that might help locate a missing child, which we provide on receipt of appropriate legal process. In just 1 week last February, we helped authorities in Fairfax, Virginia and Menlo Park, California find and return two missing kids. Last July, we received a request for IP data and basic user information for a minor who had gone missing. Over the course of the next week, we worked closely with law enforcement over e-mail and by telephone. Ultimately, the minor was found using the exact IP data we had provided. Similarly, a Facebook user went missing in Canada, and a demand for ransom was made. The Royal Canadian Mounted Police contacted us, and we followed our procedure for imminent threats. When a message was sent to a friend from the missing person's account, we provided the necessary data, enabling the RCMP to locate and return the person to safety.

Preface: only a tiny fraction of a single percent of users will ever encounter the following two kinds of behaviors on Facebook. We focus on these areas because we take any threat to our users' safety very seriously.

Registered Sex Offenders Attempting to Establish Accounts

Although it is not required to do so by law, Facebook prohibits access to Facebook by Registered Sex Offenders (RSOs). Facebook employs an outside contractor—at our own expense—to collect a list of RSOs from all of the states periodically throughout each year. Every state and locality keeps their list of RSOs in a different file format with different information and different character fonts. etc. We periodically compare that compilation of names to our user list; we do not wait for law enforcement to request that we do so. Our internal team of investigation professionals evaluates any potential matches more fully. If we find that someone on a sex offender registry is a likely match to a user on Facebook, we notify law enforcement and disable the account. On occasion, law enforcement has asked us to leave the accounts active so that they may investigate the user further.

We have worked proactively to establish a publicly available national database of registered sex offenders that enables real-time checks and includes important information like e-mail addresses and IM handles.

Child Pornography

Facebook takes substantial steps to stop any trafficking of child sexual exploitation materials, commonly referred to as child pornography. We use automated tools to automatically prohibit any sharing of known links (*i.e.,* URLs) containing these materials so that these links cannot be distributed across our service. Facebook has a highly trained team dedicated to responding to the rare occasions when child pornography is detected on the service. That team sends incident reports to the National Center for Missing and Exploited Children (NCMEC) and the U.S. Department of Justice for potential prosecution. When we encounter what we believe are new offending URLs, we deploy a new technology we have developed that enables us to pull down any URL shared throughout our service even though it has been distributed.

Facebook Innovation 6: Facebook Has Made a Commitment to Collaborate on the Advancement of Safety Online

Although Facebook has important responsibilities in advancing safety online, Facebook recognized the importance of collaborating with others to innovate in this area. Facebook has developed deep, ongoing relationships with child safety and security experts. In December, Facebook formalized these relationships by creating a Safety Advisory Board of outside experts who advise us, and, on occasion, our users about how to keep teens safe online. Facebook also continues to work closely with law enforcement agencies around the country, and around the world. We are particularly proud of our work with the States' Attorneys General. In 2008, Facebook actively participated in the Internet Safety Technical Task Force at the behest of the Attorneys General to examine these issues. In April, we launched our new Safety Center to provide our users, parents and educators with updated educational materials and information about how to utilize our innovative privacy and security tools to enhance online safety.

Conclusion: Facebook Will Continue to Innovate but Congress must Help

Although we are not a service that is directed at children less than 13 years of age, we have built our service, policies, and tools with COPPA in mind. Our experience tells us that Congress need not amend COPPA at this time. In fact, any amendments might undo many of our innovative privacy and safety tools. Congress can, however, assist Facebook and companies like us in advancing online child and teen safety by providing incentives, not disincentives, for child safety innovation online. If COPPA is amended, Congress could consider permitting companies to explore innovative approaches to obtaining parental consent online. Congress should ensure regulators are not discouraging technological and policy innovation in this area when reviewing privacy and security policies of companies that are trying to do the right thing.

We thank this subcommittee for its leadership and call on Congress to take these actions to enhance child online safety. Thank you for your consideration.

Senator PRYOR. Thank you.

Mr. Hintze?

STATEMENT OF MICHAEL D. HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Mr. HINTZE. Chairman Rockefeller, Chairman Pryor, Ranking Member Wicker, thank you for the opportunity to share Microsoft's views on the Children's Online Privacy Protection Act.

Microsoft has a deep and long-standing commitment to protecting the privacy of consumers, including children, who use our software and services. I want to begin by discussing Microsoft's comprehensive approach to protecting children's privacy online. I will then identify those areas where COPPA has made progress over the last decade, and highlight a couple of key challenges that remain.

This hearing is timely. Ten years ago, this month, the Federal Trade Commission's COPPA rule took effect. COPPA's stated goal is to preserve the interactivity of children's experience on the Internet, while protecting their privacy. That goal remains essential today. Research has found that children gain important educational and social benefits, such as increased opportunities for learning and creativity, by engaging in interactive activities online. And children are realizing these benefits as they increasingly use new technologies to access the Internet, including mobile phones, videogame consoles, and portable media players. But, as we all recognize, these interactive technologies often enable consumers to disclose personal information online, and children may not fully understand the terms or the tradeoffs involved.

COPPA was designed to address this issue. Microsoft fully supports COPPA's objectives of enhancing parental involvement and protecting children's privacy.

While children's use of the Internet has evolved over the last decade, these objectives remain just as, if not more, important today. Privacy failures can have a real impact on children's safety.

Therefore, Microsoft takes a number of steps to help protect children's privacy and safety through our own products and services, educational initiatives, and partnerships.

First, Microsoft requires parental consent and offers parental controls for a number of our products and services, including Xbox, Hotmail, and our Instant Messenger Service. For example, our Windows Live Family Safety tool enables parents to limit their children's searches, block or allow websites based on the type of

content, restrict with whom the child can communicate, and access detailed activity reports that show the websites their children visited, and the games and applications they used.

Second, Microsoft engages in educational efforts around the world to help parents and caregivers make informed decisions about children's Internet use.

Third, Microsoft partners with government officials, industry members, law enforcement agencies, and child advocates, to address children's privacy and safety issues.

The attachment to my written testimony provides more details on these initiatives.

Now I'd like to spend a few minutes talking about COPPA.

In the past decade, COPPA has made important progress in raising awareness of children's privacy issues. For example, many website operators now limit the amounts and types of information they collect from children, and provide parents and children with educational resources to foster conversations about online privacy and safety. Also, by encouraging website operators to be more transparent about their privacy practices, and encouraging them to implement parental consent mechanisms, COPPA has enabled parents to take a more active and informed role in deciding how their children can take advantage of the Internet's many benefits.

We believe COPPA provides a flexible notice-and-consent framework that can accommodate children's evolving use of new technologies. Therefore, we do not believe that a legislative amendment is necessary at this time. Rather, the statute enables the FTC to update its rule. And we appreciate the FTC's efforts to review its implementation of COPPA in light of new business models and new technologies.

I'd like to highlight two aspects of the FTC's rule that we urge the Commission to consider as part of its review.

First, the Commission should provide clear guidance on how companies can better meet, not only the letter, but the spirit of the law. Microsoft goes beyond the letter of the law by proactively requesting age information and seeking parental consent for children's use of many of its services, even when those services are not specifically targeted to children. We take this approach to encourage parental involvement in children's online activities, and enable children to participate in, and benefit from, interactive activities online. Other companies take different approaches. We encourage the Commission to use its COPPA rule-review process as an opportunity to help website operators and online services understand how they can honor the spirit of COPPA, especially in light of new technologies.

Second, we urge the Commission to work with technology companies and consumer advocates to develop more consumer-friendly, effective, and scalable methods for obtaining parental consent. The FTC has explicitly approved five parental consent methods for the disclosure of children's information online. However, these methods can be cumbersome for parents, do not scale for widely used services, and rely on children's self-reporting of age. These issues become more pronounced as children increasingly access services through mobile devices, where providing notice and obtaining parental consent raise additional challenges.

Microsoft recognizes that the task of improving the parental consent process is not easy, and there's no silver-bullet solution. The FTC's ongoing COPPA rule review provides a good opportunity for productive dialogue on alternative parental consent methods. We are committed to working, both in the short and long term, with Congress, the Commission, and other stakeholders to address privacy challenges raised by new technologies.

Thank you for the opportunity to testify today.

[The prepared statement of Mr. Hintze follows:]

PREPARED STATEMENT OF MICHAEL D. HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Chairman Pryor, Ranking Member Wicker, and honorable members of the Subcommittee, thank you for the opportunity to share Microsoft's views on children's privacy issues raised by new technologies and the Children's Online Privacy Protection Act (COPPA). Microsoft has a deep and long-standing commitment to protecting the privacy of consumers, including children, who use our software and services. We appreciate your initiative in holding this hearing today.

This hearing is timely. Ten years ago this month the Federal Trade Commission's COPPA Rule took effect. At the time, COPPA's stated goal was to preserve "the interactivity of children's experience on the Internet."[1] That goal remains essential today. Research has found that children gain important educational and social benefits, such as increased opportunities for learning and creativity, by engaging in interactive activities online.[2] And children are realizing these benefits as they increasingly use new technologies to access the Internet, including mobile phones, video game consoles, and portable media players.[3]

But, as we all recognize, these interactive technologies often enable consumers to disclose personal information online, and children may not fully understand the terms or the trade-offs involved. COPPA was designed to address this issue. Microsoft fully supports COPPA's objectives of enhancing "parental involvement in a child's activities" and protecting "children's privacy by limiting the collection, [use, and disclosure] of personal information from children without parental consent."[4] While children's use of the Internet has evolved over the last decade, these objectives remain just as—if not more—important today. Privacy failures can have a real impact on children's safety. Therefore, Microsoft has developed strong privacy practices regarding how children's personal information is collected, used, and disclosed online.

Today, I want to begin by discussing Microsoft's comprehensive approach to protecting children's privacy online. I then will identify those areas where the COPPA Rule has made progress over the last decade and highlight a couple of key challenges that remain. My testimony concludes by describing promising identity management and privacy enhancing tools that can help address these challenges.

Microsoft's Comprehensive Approach to Addressing Children's Privacy

Microsoft takes a number of steps to help protect children's privacy and safety through our own products and services, educational initiatives, and partnerships.

First, Microsoft requires parental consent and offers parental controls for a number of our products and services. For example, our Xbox Live, Spaces, Messenger, and Hotmail services request age information in a neutral manner during the registration process. If a child indicates he or she is under the age of 13, we seek and

---

[1] 144 Cong. Rec. S12787 (1998) (statement of Sen. Bryan); *see also* 64 Fed. Reg. 59888, 59889 (1999) ("In drafting this final rule, the Commission has taken very seriously the concerns expressed about maintaining children's access to the Internet.").

[2] *See, e.g.,* Carly Shuler, Joan Ganz Cooney Center at Sesame Workshop, *Pockets of Potential: Using Mobile Technologies To Promote Children's Learning* 13–14, App. A, B (2009), *http://www.joanganzcooneycenter.org/pdf/pocketsofpotential.pdf*; National School Boards Association, *Creating & Connecting: Research and Guidelines on Online Social—and Educational—Networking* 1 (July 2007), *http://www.nsba.org/SecondaryMenu/TLN/CreatingandConnecting.aspx*.

[3] According to the Henry J. Kaiser Family Foundation, children 8- to 10-years old spend about 30 minutes each day browsing websites, posting to social networking sites, and sending instant messages and e-mails to friends and family. This number more than doubles for older children. *See* Henry J. Kaiser Family Foundation, *Generation M*[2]: Media in the Lives of 8- to 18-year-olds 20 (2010), *http://www.kff.org/entmedia/upload/8010.pdf*.

[4] 144 Cong. Rec. S12787 (1998) (statement of Sen. Bryan).

obtain parental consent before the child is permitted to participate in interactive activities offered by these services.

In addition, our parental controls for Windows 7, Windows Live, Xbox 360, Zune, and other services help parents make granular choices about how their children may share personal information online. For example, our Windows Live Family Safety tool enables parents to limit their children's searches; block (or allow) websites based on the type of content; restrict whom their children can communicate with in Windows Live Spaces, Messenger, or Hotmail; and access detailed activity reports that show the websites their children visited and the games and applications they used.[5] Importantly, we have designed our family safety settings such that the settings can roam across different types of devices through which children may access these online services.

Second, Microsoft engages in educational efforts around the world to encourage parents and caregivers to talk to their children about online privacy and to assist them in making informed decisions about their children's Internet use. For example, Microsoft provides parents with a number of educational resources to help them preserve their children's privacy and protect their children from inappropriate content, conduct, and contact online.[6] And Microsoft works to raise awareness of children's privacy and safety issues by sponsoring roundtables with local and regional policymakers, academics, the media, and other thought leaders.

Third, Microsoft partners with government officials, industry members, law enforcement agencies, and child advocates to address children's privacy and safety issues. For example, we support *GetNetWise.org,* which offers parents and children resources for making informed decisions about Internet use. We also are an active participant in the National Cyber Security Alliance and its online website Stay Safe Online, which encourages children and parents to discuss topics such as disclosing personal information through Internet chat rooms, e-mail, and websites. In addition, Microsoft works closely with the International Center for Missing and Exploited Children, Interpol, the National Center for Missing and Exploited Children, and many other organizations on child protection issues.[7]

The COPPA Rule 10 Years Later

In the past 10 years, the FTC's COPPA Rule has made important progress in raising awareness of children's online privacy issues. For example, many website operators now limit the amounts and types of personal information they collect from children online and provide parents and children with educational resources to foster conversations about online privacy and safety. Also, by encouraging website operators to be more transparent about the types of personal information that they collect from children online and about the use and disclosure of this information, the COPPA Rule has enabled parents to take a more active and informed role in deciding how their children can take advantage of the Internet's many benefits.

We appreciate the FTC's efforts to review its implementation of COPPA in light of changes in technology, and Microsoft looks forward to participating in this process. While we recognize that changes to the COPPA Rule may be warranted, we do not believe that a legislative amendment is necessary at this time. COPPA provides a flexible notice and consent framework for the collection, use and disclosure of children's personal information, and we believe the statute enables the FTC to update its Rule as technologies and children's use of new technologies evolve over time.

Today, I want to highlight two key aspects of the FTC's Rule that we believe the Commission should consider as it reviews its Rule in light of new technologies.

First, we hope that the Commission will provide clear guidance on how companies can better meet not only the letter, but also the spirit, of the law in light of changing technologies and the evolving ways in which children are consuming online services. As expected, website operators and online services have adopted different approaches to complying with the COPPA Rule.[8] For example, Microsoft proactively requests age information and seeks parental consent for children's use of many of its services even when those services are not specifically targeted to children. We take this approach in order to encourage parental involvement in children's online activities and enable children to participate in and benefit from interactive activities

---

[5] *See* Attachment. Because we believe that consumers should be notified that they are being monitored to prevent abuse, children are provided on-screen notice where these tools provide parents with monitoring capabilities and these capabilities are engaged.

[6] *See, e.g.,* http://www.microsoft.com/protect/family.

[7] *See, e.g.,* http://www.microsoft.com/protect/community.aspx; Microsoft Corp., *PhotoDNA: Putting Microsoft Technology To Work Ensuring a Childhood for Every Child* (2009), *http://www.microsoftphotodna.com/*.

[8] Microsoft supports, for example, the FTC's approach of treating operators of general audience sites differently from operators whose sites are directed to children.

online. Other companies take different approaches. While flexibility in implementing the requirements of COPPA is desirable given the diverse array of websites and online services available, new technologies challenge COPPA's goal of promoting opportunities for discussions between parents and children about the disclosure of personal information online. We encourage the Commission to use its COPPA Rule review process as an opportunity to help website operators and online services understand how they can honor the spirit of COPPA, especially in light of new technologies.

Second, we urge the Commission to work with technology companies and consumer advocates to develop more consumer-friendly, effective, and scalable methods for obtaining parental consent. The COPPA Rule generally requires that website operators and online services obtain verifiable parental consent before knowingly collecting, using, or disclosing children's personal information online.[9] The FTC has appropriately adopted a "sliding scale" approach to parental consent. However, the FTC has only explicitly approved five parental consent methods for the disclosure of a child's personal information online: (1) providing a form for the parent to print, sign, and mail or fax back to the company; (2) requiring the parent to use a credit card in connection with a transaction; (3) maintaining a toll-free telephone number staffed by trained personnel for parents to call; (4) obtaining a digital certificate using public key technology; and (5) requiring an e-mail accompanied by a PIN or password obtained through one of the first four verification methods. These methods can be cumbersome for parents, do not scale for large organizations, and rely on children's self-reporting rather than an online age verification system.[10] These issues become more pronounced as children increasingly access online services through mobile devices, where providing notice and obtaining parental consent raises additional challenges.

For this reason, Microsoft recommends that the Commission expand its list of approved parental consent methods to include other reliable approaches that minimize burdens on parents, leverage existing technologies, and scale for millions of users. In addition, as more online services are made available on mobile phones and other mobile devices, the Commission should consider the types of parental consent mechanisms appropriate for these devices.

Microsoft recognizes that the task of improving the parental consent process is not easy and that there is no "silver bullet" solution. But the FTC's ongoing COPPA Rule review provides a good opportunity to begin a productive dialogue on how to take advantage of existing services and new technologies to develop alternative parental consent methods.

For example, Microsoft and others in the industry have been working on new technologies for authentication and identity management generally, and these technologies could be used to help streamline and make more effective parental consent processes.[11] Digital identity cards are one of these technologies. They could be issued through existing offline processes where in-person identity verification of a parent-child relationship already occurs. Once a digital identity card has been issued, website operators and online service providers could obtain parental consent by requesting that parents and children provide their digital identity cards before accessing interactive services and features.

Microsoft appreciates that these stronger authentication and online identity technologies can themselves impact privacy. For this reason, we believe that these systems should work in tandem with technologies that enable users to limit the personal information they disclose. For instance, Microsoft is working on technology that relies on cryptographic protocols and tokens to enable parents and children to better manage their identities online in a privacy enhancing way. When combined with the use of digital identity cards, these technologies could allow parents and children to disclose only that information that is necessary (such as parental status or age, but not name or other personal information) to enable children's access to and use of websites and online services.[12]

These identity management technologies offer exciting prospects for creating a broader range of meaningful parental consent methods tailored to the use of chil-

---

[9] 16 C.F.R. § 312.5.

[10] Children in the upper age range covered by COPPA may be sophisticated enough to provide false age information in order to access online sites and services that screen for age.

[11] *See* Microsoft Corp., *Digital Playgrounds: Creating Safer Online Environments for Children* (2008), *http://download.microsoft.com/download/2/8/4/284093f4-5058-4a32-bf13-c12e2320cd73/Digital%20Playground.pdf*; Scott Charney, Vice President Trustworthy Computing, Microsoft, "The Evolution of Online Identity," 7 IEEE SECURITY AND PRIVACY 56–59 (2009).

[12] Microsoft Corp., *Microsoft U-Prove Technology Release: Open Standards and Community Technology Preview* (2010), *http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx*.

dren's information online. Microsoft looks forward to working in close collaboration with the public sector and other industry members to evaluate and implement these technology tools as part of a comprehensive approach to protecting children's privacy online.

Conclusion

Thank you for the opportunity to testify today. We take our privacy obligations seriously, and we are committed to working in both the short and long term with Congress, the Commission and other stakeholders to address privacy challenges raised by new technologies.

ATTACHMENT

Family Safety

Helping to Protect Children in the Online World

This white paper is for informational purposes only. Microsoft Makes No Warranties, Express or Implied, in this Document.© 2008 Microsoft Corp. All rights reserved

Introduction

For children, the Internet is both a classroom and a virtual playground—a place to learn, connect with friends and have fun. But as kids explore and interact online, they might encounter content their parents would not want them to see, or they might come into contact with people who pose a threat to them. Just as there are places and activities in the physical world that are unsafe or inappropriate for children, there are places and activities online that can pose a risk to children's privacy and personal safety.

In the United States, 71 percent of teens with online access have a social networking profile.[1] Half of all British children aged 12 to 18 use instant messaging.[2] Among Australian children who use the Internet, 75 percent visit video-sharing websites and 95 percent play games online.[3] In Brazil, 98 percent of children with online access download music.[4] Children don't always apply the common-sense personal boundaries and social mores of the offline world to their online experiences. In this context, today's parents consider the Internet the greatest risk to their children among all types of media, according to one study.[5]

Parents and caregivers are in the best position to make decisions about what is appropriate for children and to talk to them about online safety. But they need help, particularly through tools and guidance. Microsoft has invested significantly in family safety online, incorporating family safety features into a broad range of Microsoft products and services that are available for consumer use. At the same time, we have made extensive efforts—often in collaboration with child development experts and non-profit partners—to provide guidance and education for teachers, parents and children. We also work with law enforcement, industry partners and governments to combat Internet crime and to strengthen legislation that protects children from online exploitation.

Making the Internet safer for children aligns with Microsoft's overall commitment to increasing trust and safety online and to protecting consumer security and privacy. (See sidebar on page 2.) Our efforts to promote family safety in the digital world fall into three key areas:

- *Tools and technology*. Microsoft offers family safety settings and parental controls in Windows Vista®, Windows Live™, Xbox 360®, Xbox LIVE®, Zune® and other products and services. We are also an industry leader in developing interoperable technologies for identity management and tools that independent software vendors can use to extend the safety capabilities of the Windows Vista platform.

---

[1] Cox Communications Teen Internet Safety Survey, Wave II—in Partnership with the National Center for Missing & Exploited Children (NCMEC) and John Walsh, March 2007. *http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt*. A social networking profile is a user's personal page on a social networking website. Profiles often include information about the person, photos, videos, personal blogs and contact information.

[2] "A European Research Project: The Appropriation of New Media by Youth." Mediappro, 2006. *http://www.mediappro.org/publications/finalreport.pdf*.

[3] "Norton Online Living Report. Symantec, 2008. *http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/nolr/080214_aus_norton_online_living_report_nolr-final.pdf*.

[4] *Ibid*.

[5] Common Sense Media Parents Study, Insight Research Group, May 19, 2006. *http://www.commonsensemedia.org/news/CS-Parent-Study.PPT*.

Guidance and education. Microsoft works with governments, nonprofits and community organizations to help parents and children better understand online risks and how to reduce them. These efforts range from informational websites and Internet safety curricula to public-information campaigns.

Law enforcement and public policy. Microsoft works with law enforcement agencies and other partners to offer tools and training that aid law enforcement efforts to apprehend and prosecute criminals who use the Internet to harm children. We also support government efforts to craft and enact effective public policies that help protect Internet users and penalize online criminals.

Security and Privacy at Microsoft

Consumer security and safety are a top priority for Microsoft. Six years ago, the company launched its Trustworthy Computing Initiative, a company-wide top-to-bottom commitment to delivering secure, private and reliable computing experiences for everyone. In addition to improved software development practices, Trustworthy Computing includes support for strong laws addressing criminal online conduct; support for law enforcement training, investigations, coordination and prosecutions; and guidance for customers on adopting security and privacy best practices.

Our corporate privacy policies—including a set of privacy principles released in 2007 related to search and online advertising—reflect our long-held commitment that consumers should have the ability to control the collection, use and disclosure of their personal information.[6] This is nowhere more crucial than in the area of young people's Internet use. From social networking sites to e-mail to online gaming, responsible user practices and technology safeguards must be applied to help keep young Internet users—and their personal information—safe.

Technology

When it comes to children's safety online, there is no technological silver bullet that can substitute for parental involvement, supervision and guidance. But Microsoft is committed to developing tools and technologies that can help parents in this important task. Family safety tools and features have been built into a wide range of Microsoft products and services, including Windows Vista, Windows Live, Xbox 360, Xbox LIVE, Zune and Mediaroom™.[7] These include tools that give parents greater control over what their children can access and how they can interact via the Web and elsewhere online—from Web content filtering and e-mail contact management to social networking restrictions.

Windows Vista

In all home editions of Windows Vista, Microsoft's next-generation client operating system, separate accounts can be created for each member of the family.[8] And using the centralized *Parental Controls* panel, parents can specify when their children can use the computer, which websites they can visit and which software applications they can use. Parents can also restrict access to PC software games based on title, content or rating. They can even view detailed reports about a child's computer use to look for potentially inappropriate sites that the child might be visiting.

Monitoring children's computer use not only helps parents keep track of what their kids are seeing, hearing and doing, but it enables them to refine and modify restrictions based on actual feedback and offers a basis for informed discussion with their kids about Internet use and online habits. The Parental Controls icon in the system tray is always visible to let children know that the Parental Controls feature is on.

For Web content filtering, parents can create customized settings that block sites by type of content (such as mature content, pornography or sex education) or specifically allow only certain sites. Parents can also enable a setting that prevents children from downloading software.

---

[6] Details on Microsoft's privacy policies are available at *http://privacy.microsoft.com/*.

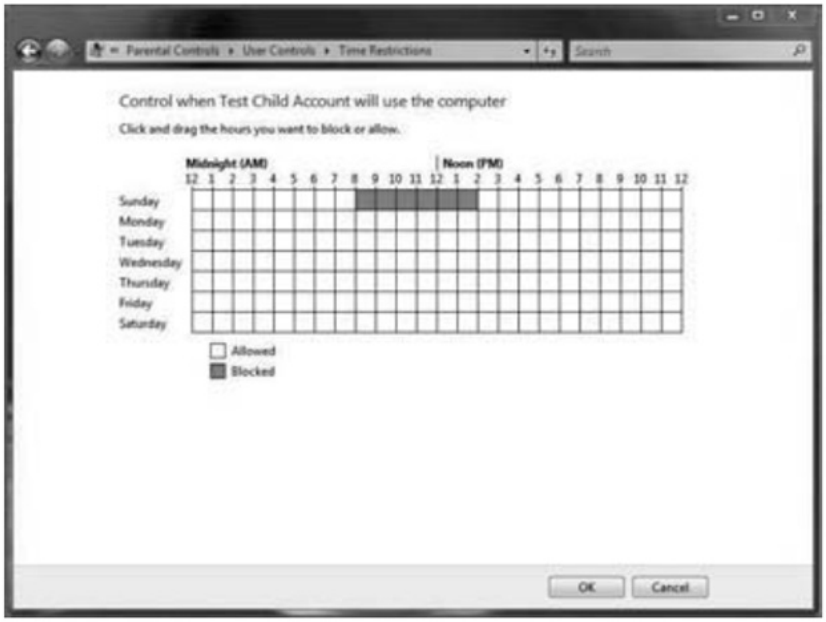
[7] More information on these and other family safety technologies can be found at *www.microsoft.com/protect.*

[8] The Starter, Home Basic, Home Premium and Ultimate editions.

To restrict the amount of time kids spend using the computer, parents can use a simple point-and-click grid to indicate "blocked" and "allowed" days of the week and hours of the day. As the end of an approved time period approaches, the child receives a 15-minute and a 1-minute notification. If the allotted time ends before the child logs off, Windows Vista suspends the session and saves all of the child's work.

From the Windows Vista Parental Controls panel, users can also enable safety features—such as content filters—that are built into third-party software and services.[9] Microsoft also offers application programming interfaces (APIs) so third-party developers can build to the Windows Vista platform.

[9] Windows Vista Parental Controls are configured to turn themselves off to prevent conflicts with third-party family safety applications.



Windows Media Center

Windows Media Center in Windows Vista Home Premium and Ultimate editions is a feature that allows you to watch and record live TV on your computer. It includes Parental Controls that let parents restrict viewing of digital entertainment by industry ratings (including the Motion Picture Association of America). Parents can:

- Set a maximum allowed rating for television and movie content (such as PG–13 or TV–14)
- Restrict access to unrated programming
- Block access to programming based on category: fantasy violence, suggestive dialogue, offensive language, sexual content or violence

Windows Live

Windows Live (*http://get.live.com*) is a set of free Web services and PC applications that help people stay better connected and get the most out of their Windows experience. It includes the Windows Live Hotmail e-mail client, social networking with Windows Live Spaces, instant messaging with Windows Live Messenger and other services.

A key offering of Windows Live is *Windows Live OneCare™ Family Safety*, a service that seamlessly integrates family safety options for Windows Live services. Family Safety offers adjustable content filtering, activity reports for each user in the family, and contact management features to help prevent children from interacting with unknown individuals. Parents can monitor online activity and update settings from any Internet-connected computer.

Family Safety also includes expert guidance for parents on age-appropriate settings. For certain markets, this guidance is country-specific. For example, the U.S. version of Family Safety includes guidance from the American Academy of Pediatrics; in Germany, the guidance is from Deutsches Kinderhilfswerk.

Family Safety can be used with Windows XP SP2 and later versions of the Windows® operating system, and it supports Windows Internet Explorer® 6 and later versions, as well as other browsers. Key elements of the service include:

Contact management. Online contact with strangers is a significant concern for parents because of the potential for harassment, inappropriate online interaction and contact with predators. Parents can specify that their approval be required before their child can communicate with a new person using Windows Live services such as Windows Live Hotmail and Messenger or before a new person is allowed to see the child's social networking page or blog on Spaces. The contact-management settings apply even when a child logs on to Windows Live from a computer outside the home.

- *Content filtering.* Parents can specify unique filtering settings for each member of the family. These settings allow, block or display a warning for a range of content categories, which apply to all Web content viewing. Filtering guidance helps parents determine age-appropriate settings and online activities as well as how to talk to children about safe Web browsing practices.

In addition, abuse reporting is available throughout Windows Live and the MSN* network of Internet services so users can report inappropriate behavior or content.[10]

Other major Windows Live services also have their own specific safeguards and privacy tools. They allow users to do the following:

Live Search

- Filter search results for sexually explicit images and text

[10] For example, there is a Report Abuse button at the bottom of every Windows Live Space so customers can easily report issues.

Windows Live Messenger

- Create a manually selected list of allowed instant messaging contacts
- Be notified whenever someone tries to add you to their Messenger Contacts list
- Block a person from contacting you or seeing if you are online

Windows Live Hotmail

- Set your personal account filters so Windows Live Hotmail will deliver mail only from people on your Contacts list and trusted senders
- Block all e-mail from a particular e-mail address
- Identify, based on color-coded alerts, whether an incoming message might be malicious or fraudulent

Windows Live Spaces

- Make your Windows Live Space completely private, available only to selected people, or public
- Access safety information from any Spaces page

Xbox 360 and Xbox LIVE

Xbox 360 and Xbox LIVE—Microsoft's gaming platform and online gaming environment, respectively—are designed to provide secure gaming and age-appropriate content for all users. The easy-to-use Family Settings console in Xbox 360 allows parents to set restrictions that apply to both offline and online play.

The console recognizes game and video rating systems from countries around the world, allowing parents to specify categories of games and movies their children can access.[11] It also has a Family Timer feature that parents can use to limit the duration of game play within each 24-hour period.

For Xbox LIVE, the console can be configured to allow online gaming and communication only with approved friends and to require parental approval for new friends. It also allows users to report inappropriate use of the service.

Specifically, the Xbox 360 Family Settings console allows parents to:

- Customize each child's playing environment
- Specify how much time a child can spend playing games each day or each week
- Specify which games a child can play, based on game rating

[11] Systems for rating age-appropriateness of video and game content vary by country or by region. They include the Entertainment Software Rating Board (*www.esrb.org*) in the United States and Canada, the British Board of Film Classification (*www.bbfc.co.uk*) in the UK, the Game Rating Board (*www.grb.or.k*) in Korea, Unterhaltungssoftware Selbstkontrolle (*www.usk.de*) in Germany, and Pan-European Game Information (*www.pegi.info*) in much of Europe.

- Override parental restrictions on a case-by-case basis
- Create personal Xbox LIVE settings for a child that will apply to that account no matter what machine is used to access the account
- Require parental approval of each child's list of online friends
- Specify which types of online communication are allowed (*i.e.,* text and voice, video)
- Limit exposure to content created by other members of the Xbox LIVE community
- Limit sharing of personal profile information to friends only, or block all sharing of personal profile information

Mediaroom

Microsoft Mediaroom, the latest version of Microsoft's Internet Protocol Television (IPTV) software platform, allows cable operators and telecommunication companies to deliver content and services such as standard and high-definition TV channels, digital video recordings and video on demand.

Mediaroom includes parental control features for managing children's access to channels, shows and services. Using a PIN or multiple PINs, parents can restrict:

- Access to programming by rating (with special functionality for blocking adult-rated programming)
- Access to unrated programming
- Access to individual channels
- The ability to purchase video-on-demand and other content

Zune

Parents can use Family Settings to restrict their children's access to and ability to purchase content from the Zune Marketplace online music store for use on their Zune portable media player. Specifically, parents can:

- Specify whether a child can make purchases from Zune Marketplace.
- Restrict a child's access to explicit content available through Zune Marketplace.
- Specify who can send messages to a child in the Zune Social online community. (Children 12 and under are prohibited from joining the community.)
- Specify whether a child can accept friend requests in the Zune Social online community.
- Specify whether a child can share favorite artists and songs with the Zune community.
- Specify who can see a child's friends list.

Guidance and Education

While Microsoft continues to create tools and technologies to help promote child safety on the Internet, we believe that educating parents and children is the most effective way to respond to online risks. To this end we support numerous family safety educational organizations and outreach efforts, including:

- *Ad Council's Internet Safety Coalition (ISC).* Microsoft is a member of the ISC, which is working to help kids understand that the Internet is a public place and to explain the risks of ill-considered Internet posting.
- *Bad Guy Patrol.* As part of Microsoft Canada's and the Government of Alberta Children's Services shared commitment to preventing child sexual exploitation, *www.badguypatrol.ca* teaches children ages 5–10 critical Internet safety skills through a series of games. A section for adults provides additional tips on how to keep kids safe and the program is being offered to other provinces across Canada.
- *GetNetWise.* Microsoft supports this public education organization and website (*www.getnetwise.org*), which offer Internet users resources for making informed decisions about safer Internet use.
- *Get Safe Online.* Microsoft is a founding sponsor, along with the UK government and other leading companies, of this campaign and website (*www.getsafeonline.org*) devoted to teaching consumers and businesses about Internet security and safety.
- *i-SAFE America's i-LEARN.* Microsoft is a sponsor of this free online curriculum for educators, parents, teens and law enforcement, which is available at *www.ilearn.isafe.org*.

- *National Cyber Security Alliance (NCSA).* Microsoft is part of this nonprofit public-private partnership that offers online safety and security information to the public on the *www.staysafeonline.org* website and through educational efforts such as National Cyber Security Awareness Month.
- *NCMEC Netsmartz.* Microsoft has provided video production resources for the National Center for Missing and Exploited Children's Netsmartz website (*www.netsmartz.org*), which helps educate parents, kids, teachers and law enforcement about online security and safety issues.
- *NetSafe*. NetSafe and Microsoft New Zealand developed this online safety site (*www.hectorsworld.com*), which offers Internet safety curricula for teachers as well as a range of fun activities for children that teach them about safer Internet use.
- *OnGuard Online.* Microsoft helped develop the U.S. Federal Trade Commission's website at *www.onguardonline.gov*, which offers consumers tips, articles, videos and interactive activities related to online safety and security.
- *"Safety is no game. Is your family set?" Tour.* Microsoft, Boys & Girls Clubs of America and Best Buy cosponsored a 20-city campaign to promote safer and age-appropriate gaming and to teach kids and parents about the Xbox 360 family safety features.[12]
- *Staysafe.org.* Microsoft sponsors and finances a website at *www.staysafe.org* that offers guidance and news about online security and safety issues. In 2006, Microsoft joined with the Federal Trade Commission, AARP, U.S. Chamber of Commerce, Best Buy and other partners to sponsor Staysafe.org's Get Net Safe Tour of 12 U.S. cities to raise awareness about Internet security and safety.
- *Wired Safety.* Microsoft is helping to support Wired Safety's first international conference on cyberbullying, at which representatives from government, education, the media, the technology industry and others will help raise awareness of this important issue and spur appropriate action.

In addition to these partnerships, at our *www.microsoft.com/protect/family* website we offer our own broader information about consumer online safety in three key areas:

- *Family Safety*—With young people online in record numbers we provide families with guidance to help promote personal safety and privacy. Just as parents teach their children to look both ways before they cross the street, Microsoft is working to help parents engage with their children to apply similar safety rules to protect kids online.
- *Protect Your PC*—Helping users protect their PCs from threats like viruses and spyware is another key area of continued focus.
- *Protect Yourself*—ID Theft is a significant concern for consumers. Microsoft is actively addressing ways to help people better protect themselves when online.

Law Enforcement and Public Policy

Microsoft is committed to helping make the Internet safer for all users, especially children and families, but we can't do it alone. Partnerships with law enforcement agencies, governments, nonprofit organizations and other industry leaders are essential to combating cybercrime. Microsoft has also worked with governments to strengthen online safety and privacy laws and to develop mandatory Internet safety education programs in schools. These efforts address not only individual children's use of the Web but also broader criminal issues like online child pornography.

One highly successful effort is the *Child Exploitation Tracking System* (CETS), a system jointly developed by Microsoft and Canadian law enforcement to manage investigations of child exploitation cases. CETS allows investigators to import, organize, analyze and search large volumes of information while conducting investigations and share information across law enforcement agencies. To date, CETS has been deployed in Canada, Brazil, Chile, Indonesia, Australia, Italy, Romania and the United Kingdom.

In June 2006, Microsoft, AOL, Earthlink, United Online and Yahoo! announced a partnership with the *National Center for Missing and Exploited Children* (NCMEC) to fund a new *Technology Coalition* within NCMEC to develop and deploy technology solutions that disrupt the ability of online predators to exploit children

[12] Educational materials from the campaign, including a parent-child gaming pact that families can fill out, are available at *http://www.xbox.com/en-US/support/familysettings/isyourfamilyset/default.htm*.

or traffic in child pornography. The participating companies pledged US$1 million in combined initial funding as well as technical support and expertise.

Microsoft has worked with *Interpol* and the *International Centre for Missing & Exploited Children* (ICMEC) to sponsor worldwide training sessions for law enforcement personnel on computer-facilitated crimes against children. As of February 2008, more than 2,600 law enforcement officers from more than 100 countries have been trained in methods of identifying suspects, investigating offenses and dealing with victims of online child predators.

In 2006, Microsoft joined ICMEC, NCMEC, leading financial institutions and Internet industry leaders to form the *Financial Coalition Against Child Pornography*, which provides a forum for members to collaborate on strategies to cutoff funding for child pornographers and eradicate child pornography.

Microsoft works extensively with the U.S. Department of Justice's *Internet Crimes Against Children Task Force* and is a member of the *Virtual Global Taskforce*, a public-private partnership that combats online child abuse worldwide.

In 2008, Microsoft joined the *Internet Safety Technical Task Force*, a coalition of academics, industry, advocacy groups and others that examines issues related to Internet safety, online authentication and children's age verification.

Microsoft includes tools in its online services that can help detect and prevent child pornography and exploitation, and it is continually developing new tools both independently and in conjunction with its partners. MSN uses a filtering tool to review images uploaded to Windows Live Spaces and MSN Groups. Microsoft reports any images identified as apparent child pornography to NCMEC and closes the site. Microsoft also has a complaint center where users can report incidents of abuse on our sites.

Microsoft has worked with state attorneys general in Alabama, Colorado, Georgia, Kansas, Massachusetts, New Hampshire, New Mexico, South Carolina and Utah to provide comprehensive training for law enforcement on computer-facilitated crimes.[13]

In April 2006, Microsoft joined ICMEC in announcing ICMEC's model legislation on child pornography. This legislation seeks to modernize child pornography laws for the 184 member countries of Interpol; Microsoft has pledged to support efforts worldwide to develop and enforce these laws.

Microsoft has joined industry partners to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address crime in the online environment.

Conclusion

Microsoft has long been committed to helping protect children online. We take a comprehensive approach to online safety that includes the development of family safety technologies, guidance and education for families and children, and partnerships with industry and law enforcement to combat online crime.

Online child safety is directly in line with Microsoft's overall commitment to promoting greater trust online and to offering products and services built with consumer safety in mind. Microsoft will continue to invest in programs, technologies and partnerships that advance the goals of safe computing for children and families.

[The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Microsoft, Internet Explorer, Mediaroom, MSN, OneCare, Xbox 360, Xbox LIVE, Windows, Windows Live, Windows Vista and Zune are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The

[13] In the United States, the attorney general is the state government's chief legal advisor and law enforcement officer.

names of actual companies and products mentioned herein may be the trademarks of their respective owners.]

Senator PRYOR. Thank you.

Dr. Montgomery?

STATEMENT OF KATHRYN C. MONTGOMERY, PH.D., PROFESSOR, SCHOOL OF COMMUNICATION, AMERICAN UNIVERSITY

Dr. MONTGOMERY. Chairman Rockefeller, Chairman Pryor, Ranking Member Wicker, and members of the Committee—the Subcommittee, thanks so much for inviting me to testify about COPPA. It's a law I care very deeply about.

During the 1990s, while President of the nonprofit Center for Media Education, I played a leadership role in passage of COPPA, working with Members of Congress on both sides of the aisle, as well as a coalition of prominent education, health, and consumer groups.

And I think we need to remember that, in the early days of the World Wide Web, which was really a kind of Wild West period, the business model of one-to-one marketing, combined with the increasing value of children as a target market for advertisers, created, really, a "perfect storm" for marketers who wanted to use the Internet to take advantage of young people. We and others documented many of those practices. And if we need to remind ourselves of where we were, we can remember sites like the Young Investors site that asked for reams of personal financial information from children, or one of my favorites, which was the Batman site, which asked children to be good members of Gotham and fill out the census. That's what we were looking at, at the time. That's where the Internet was headed.

My colleagues and I consulted with a broad spectrum of stakeholders, including industry groups, to craft a set of regulations that would successfully balance our collective interest in nurturing the growth of e-commerce while protecting the privacy of our children.

And I think COPPA has served us all very well. It has created a level playing field by creating a law that applied to every online commercial player, from the largest children's media companies to the smallest startups, and it sends a signal to the industry, "If you're going to do business with our Nation's children, you will have to follow some rules." And because it was passed during the early stages of e-commerce, it has created rules of the road that have helped to guide the development of the digital marketplace and, really, curtail many of the egregious practices that were coming into place.

And I also think the Safe Harbor mechanism is very important, because it permits self-regulation, but within the context of clear government rules and enforcement authority by the FTC.

But, as others have pointed out, recent developments in online marketing really warrant renewed attention by the FTC and the Congress. Today's children are growing up in an immersive and ubiquitous digital media environment, 24/7, and many of the practices we identified in the 1990s have been eclipsed by an entirely new generation of tracking and targeting technologies. Briefly, I'll highlight two.

One is behavioral targeting, which is an invisible process and a covert process that tracks individual users, through cookies and other data files, to collect information about them, and to design personalized advertising to target them, based on their psychological profiles and their behavioral profiles. And this also raises the question of what constitutes "personally identifiable information." It's not just a matter of your giving your name. The marketers are able to know who you are, and get to you and target you.

And the second is mobile marketing, which people have mentioned. And one of the important things is that it combines behavioral targeting with location targeting. And the research that I've done on children's food marketing and the obesity crisis has found fast-food companies creating discount coupons that will be sent to people's and children's cell phones when they get near a fast-food restaurant.

So, what we need to do is to ensure the FTC—and I'm working with the agency to update the law, update the rules, as it was intended to do, as it was designed to do.

Finally, I do want to say that, while COPPA has established important safeguards for the youngest consumers in the digital marketplace, adolescents have no such protections. We know they're avid users of social networks, like Facebook and MySpace and others. In many ways, they're living their lives online, and they're increasingly relying on these social networks and on search for personal information and for handling sensitive personal issues that they're coping with in their lives.

So, I would argue, we—I'm not arguing for a parental verification system, like COPPA, but I do think we need a set of fair information and marketing practices that are tailored to the unique needs and vulnerabilities of adolescents.

So, I hope the Committee will send a message to the FTC that COPPA remains important, but needs to be updated, and also, that the FTC should develop specific recommendations for protecting the privacy of adolescents as part of its broad new initiative on online privacy.

Thank you.

[The prepared statement of Dr. Montgomery follows:]

PREPARED STATEMENT OF KATHRYN C. MONTGOMERY, PH.D., PROFESSOR, SCHOOL OF COMMUNICATION, AMERICAN UNIVERSITY

Chairman Pryor, Senator Wicker, and members of the Subcommittee. My name is Kathryn Montgomery, and I am a Professor in the School of Communication at American University. I appreciate the opportunity to testify before you today about the Children's Online Privacy Protection Act (COPPA). During the 1990s, while president of the nonprofit Center for Media Education (CME), I played a leadership role in the passage of COPPA, working with a coalition of education, health, and consumer groups that included the National PTA, the Consumer Federation of America, the National Education Association, and the American Academy of Pediatrics. As you know, Congress passed the law in 1998 through the strong bi-partisan leadership of Sen. John McCain (R–Ariz.), Rep. Ed Markey (D–Mass), and then-Sen. Richard Bryan of Nevada. I worked closely with these Congressional leaders and with other members, as well as with the Federal Trade Commission and the White House, on the legislation. I also collaborated with a broad spectrum of industry stakeholders—including advertising trade groups, online content providers, and children's media companies—to craft a statute and a set of regulations that would successfully balance our collective interests in nurturing the growth of e-commerce, while protecting the privacy of our children.

For the past decade, COPPA has served as an effective safeguard for young consumers under the age of 13 in the online marketing environment. Though the law took effect in the early formative period of Internet marketing, it was purposely designed to adapt to changes in both technology and business practices, with periodic reviews by the FTC to ensure its continued effectiveness. With the current expansion of digital media platforms and the growing sophistication of online data collection and profiling, however, it is now critically important that the intent of COPPA be fully implemented to protect young people from new commercial practices in today's digital media environment.

As I document in my book, *Generation Digital: Politics, Commerce and Childhood in the Age of the Internet*, the emergence of the World Wide Web ushered in a host of online marketing and data collection practices that raised fundamental privacy concerns for children. The business model of one-to-one marketing, combined with the increasing value of children as a target market for advertisers, created a perfect storm for marketers who wanted to use the Internet to take advantage of young people. Numerous commercial websites offered prizes and other incentives to encourage children to supply personal information about themselves. For example, one site targeted at "young investors," urged children to provide an astonishing amount of financial information, including any gifts they might have received in the form of stocks, cash, savings bonds, mutual funds or certificates of deposit. Another site, set up to promote the movie *Batman,* encouraged children to "be good citizens of Gotham" and fill out the "census." [1] Some of these practices were so disturbing that the Center for Media Education enlisted the help of Georgetown University Law Center's Institute for Public Representation to file a complaint with the FTC in 1996. The commission found our complaint persuasive and, with the urging of our coalition and others, began examining the children's online data collection commercial market.[2] The FTC's internal research played a key role in documenting the rampant spread of data collection and the failure of self-regulatory promises by industry. The commission's report, released just months prior to passage of COPPA, provided crucial evidence of the need for this important law.[3]

Congress made a wise decision in 1998 to enact COPPA. I believe the law has been a clear legislative success. It was a balanced and sensible solution to a challenging problem. It established a level playing field by creating a law that applied to every commercial player—from the largest children's media companies to the smallest startups. And it sent a strong signal to the growing online marketing industry: If you are going to do business with our Nation's children, you will have to follow some basic rules. Because decades of research documented younger children's particular vulnerabilities to advertising and marketing, the law was narrowly tailored to apply only to commercial websites that were targeted at children under the age of 13, or where there was actual knowledge by the website operator that the user was under that age. In keeping with fair information principles, a key intent of the law was to minimize the collection of personally identifiable data from children, and to eliminate the practice of offering prizes and other incentives to encourage such data collection.[4]

No law is perfect, as everyone in this body is well aware. In the case of COPPA, children who are under 13 can lie about their age when visiting sites that are not intended for them. Parents are not always willing or able to be involved in the day-to-day online navigations of their children. But because the legislation was passed during the early stages of Internet e-commerce, COPPA established a clear set of "rules of the road" to help guide the development of the children's digital marketplace. As a result, some of the most egregious data collection practices that were becoming state-of-the-art in the online marketing environment were curtailed. A

---

[1] Kathryn Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: MIT Press, 2007); Kathryn Montgomery and Shelly Pasnik, *Web of Deception: Threats to Children from Online Marketing* (Washington, D.C.: Center for Media Education, 1996).

[2] Federal Trade Commission, "FTC Staff to Survey Consumer Privacy on the Internet," 26 Feb. 1998, *http://www.ftc.gov/opa/1998/02/webcom2.shtm*; Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2000, *www.ftc.gov/reports/privacy2000/privacy2000text.pdf* (both viewed 26 Apr. 2010).

[3] Federal Trade Commission, "Privacy Online: A Report to Congress," June 1998, *http://www.ftc.gov/reports/privacy3/priv-23a.pdf* (viewed 26 Apr. 2010).

[4] The FTC's COPPA rule applies to "Operators of commercial websites and online services directed to children under 13 that collect personal information from them; operators of general audience sites that knowingly collect personal information from children under 13; and operators of general audience sites that have a separate children's area and that collect personal information from children under 13." Federal Trade Commission, "Children's Online Privacy Protection Act," *http://www.ftc.gov/privacy/privacyinitiatives/childrens.html* (viewed 26 Apr. 2010).

study in the *Journal of Consumer Affairs* found that more than ninety-five percent of the top 100 children's websites in the United States post privacy policies complying with COPPA's requirements for information collection and use.[5] And by establishing a safe -harbor mechanism, the law created a system whereby self-regulatory guidelines—developed and implemented by a number of entities—operate within a framework of clear government rules and enforcement authority by the FTC. We are pleased that the commission has taken the initiative to examine and respond to specific cases, cracking down on those practices that violated the statute.[6]

Recent developments in the online marketing arena, however, pose new challenges that warrant the attention of the FTC and Congress. The Web has matured, thanks especially to broadband and mobile technologies. As a result, not only has the digital marketplace grown dramatically, it has become an even stronger presence in the lives of young people. Today's children are growing up in a ubiquitous digital media environment, where mobile devices, instant messaging, social networks, virtual reality, avatars, interactive games, and online video have become ingrained in their personal and social experience. Members of this generation of young people are, in many ways, living their lives online. As *Advertising Age* reported, "more than 16 million children aged 2 to 11 are online, making for a growth rate of 18 percent in the period 2004 to 2009—the biggest increase among any age group, according to Nielsen." The same report explains that according to a Nielsen Online survey conducted in July 2009, "Time spent online for children ages 2 to 11 increased from about 7 hours to more than 11 hours per week, or a jump of 63 percent over 5 years."[7]

The online marketing practices we originally identified in the 1990s have been eclipsed by a new generation of tracking and targeting techniques. For example, mobile marketing—combining text messaging, mobile video, and other new applications—is one of the fastest growing digital commerce platforms throughout the world, and a particularly effective way to reach and engage children.[8] As a recent Kaiser Family Foundation study noted, "Over the past 5 years, there has been a huge increase in [cell phone] ownership among 8- to 18-year-olds: from 39 percent to 66 percent. . . . During this period, cell phones . . . have become true multimedia devices: in fact, young people now spend more time listening to music, playing games, and watching TV on their cell phones (a total of :49 daily) than they spend talking on them (:33)."[9] According to the latest industry data, roughly half of all children use a mobile phone by age 10, and by age 12, fully three-fourths of all children have their own mobile phone.[10] As one media executive commented, the mobile phone is "the ultimate ad vehicle . . . the first one ever in the history of the planet that people go to bed with."[11] Mobile advertising will increasingly rely on interactive video and become firmly embedded in "mobile social networks." Advertising on mobile devices will be especially powerful, since it will be able to target users by combining both behavioral and location data.[12] Ads on mobile phones will

---

[5] Anthony D. Miyazaki, Andrea J. S. Stanaland, and May O. Lwin, "Self-Regulatory Safeguards and the Online Privacy of Preteen Children, *Journal of Advertising* 38, n. 4 (Winter 2009): 79, 83; Andrea J. S. Stanaland, May O. Lwin, and Susanna Leong, "Providing Parents with Online Privacy Information: Approaches in the U.S. and the UK," *Journal of Consumer Affairs* 42 n. 3 (Fall 2009): 474, 484–85.

[6] See for example, Federal Trade Commission, "Iconix Brand Group Settles Charges Its Apparel Web Sites Violated Children's Online Privacy Protection Act," 20 Oct. 2009, *http://www.ftc.gov/opa/2009/10/iconix.shtm* (viewed 26 Apr. 2010).

[7] Beth Snyder Bulik, "The On-Demand Generation," 12 Apr. 2010, *http://adage.com/digital/article?article_id=143220* (viewed 26 Apr. 2010).

[8] E. Burns, "U.S. Mobile Ad Revenue to Grow Significantly through 2013," *ClickZ,* 25 Feb. 2009, *http://www.clickz.com/3632919* (viewed 4 Aug. 2009).

[9] Kaiser Family Foundation, "Daily Media Use Among Children and Teens Up Dramatically from Five Years Ago," 20 Jan. 2010, *http://www.kff.org/entmedia/entmedia012010nr.cfm* (viewed 7 Apr. 2010).

[10] Pete Blackshaw, "A Pocket Guide to Social Media and Kids," Nielsen Wire, 2 Nov. 2009, *http://blog.nielsen.com/nielsenwire/consumer/a-pocket-guide-to-social-media-and-kids/* (viewed 16 Mar. 2010).

[11] A. Klaassen, "Why Google Sees Cellphones as the 'Ultimate Ad Vehicle,'" *Advertising Age*, 8 Sept. 2008, *http://adage.com/mobilemarketingguide08/article?article_id=130697* (viewed 4 Aug. 2009).

[12] Center for Digital Democracy and U.S. PIRG, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices," Federal Trade Commission Filing, 13 Jan. 2009, *http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing* (viewed 7 June 2009).

be able to reach young consumers when they are near a particular business and offer electronic pitches and discount coupons.[13]

Behavioral targeting uses a range of online methods—including cookies and invisible data files—to learn about the unique interests and online behaviors through the tracking and profiling of individual users. Through a variety of new techniques, marketers use this data to create personalized marketing and sales appeals based on a customer's unique preferences, behaviors, and psychological profile.[14] Recent advances in behavioral targeting are enabling marketers to more accurately predict and influence user behavior. For example, "predictive behavioral targeting" combines data from a number of different sources and makes inferences about how users are likely to behave in their response to marketing messages. Increasingly, behavioral profiles incorporate information from outside databases.[15] Social media platforms are also embracing behavioral targeting, helping to drive "robust advertising response and conversion."[16]

Last year, a broad coalition of consumer, children, and privacy groups urged the FTC to ensure that new technologies involving mobile phones and data collection incorporate COPPA relevant safeguards. These groups also want the FTC to determine how behavioral marketing impacts children covered by COPPA, by analyzing, for example, the stealth data collection process delivered by online games, virtual worlds, and age-relevant social sites.[17] In its current review, the commission must ensure that its regulations implementing COPPA include the full range of Internet -enabled or connected services, including the increasingly ever-present cell phones children use, along with Web-connected gaming devices and online, interactive video.[18] Congress intended COPPA's basic framework to be flexible, anticipating that the FTC would have to ensure that the law's implementation would cover new ways of collecting personal information from children.[19] That's why I strongly support the FTC asking, in its recent *Federal Register* notice, whether COPPA's definition of personal information should be revised to include the latest methods of identifying and targeting online consumers, covering the so-called "cookies" that are used for interactive marketing data collection, as well as "mobile geo-location information."[20] As the February 2009 FTC staff report on online privacy acknowledged, "in the context of online behavioral advertising, the traditional notion of what constitutes PII [personally-identifiable information] versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for

---

[13] A. Johannes, "McDonald's Serves Up Mobile Coupons in California," *PROMO Magazine*, 26 Oct. 2005, *http://promomagazine.com/incentives/mcds_coupons_102605/* (viewed 4 Aug. 2009).

[14] David Hallerman, "Behavioral Targeting: Marketing Trends," eMarketer, June 2008; I. Khan, B. Weishaar, L. Polinsky, *et al.*, "Nothing but Net: 2008 Internet Investment Guide," 2008, *https://mm.jpmorgan.com/stp/t/c.do?i=2082C248&u=a_p*d_170762.pdf*h_-3ohpnmv* (viewed 23 Mar. 2009).

[15] "About Acxiom," *http://www.acxiom.com/about_us/Pages/AboutAcxiom.aspx* (viewed 7 June 2009).

[16] "ValueClick Media Launches Predictive Behavioral Targeting," 21 July 2008, *http://phx.corporate-ir.net/phoenix.zhtml?c=84375&p=irol-newsArticle&ID=1177051*; Acxiom, "Digital Marketing Services," *http://www.acxiom.com/products_and_services/digital/Pages/DigitalMarketingServices.aspx*; "24/7 Real Media Launches Social Media Targeting to Improve Ad Performance and Response," 27 Apr. 2009, *http://www.247realmedia.com/EN-US/news/article_445.html* (all viewed 7 June 2009).

[17] "Comments of American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, the American Psychological Association, Benton Foundation, Campaign for a Commercial Free Childhood, Center for Digital Democracy, Children Now, and the Office of Communications of the United Church of Christ. Online Behavioral Advertising Principles," Federal Trade Commission filing, 11 Apr. 2009, *http://www.democraticmedia.org/news_room/letters/Letter_re_behavioral_advertising_comments*; Center for Digital Democracy and U.S. PIRG, filing with the Federal Trade Commission concerning "Online Behavioral Advertising Principles," 11 Apr. 2008, *http://www.democraticmedia.org/files/FTCfilingApr08.pdf*; Federal Trade Commission Staff Report, "Beyond Voice, Mapping the Mobile Marketplace," Apr. 2009, 3 *http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf* (all viewed 26 Apr. 2010).

[18] Federal Trade Commission, "FTC to Host Public Roundtable to Review Whether Technology Changes Warrant Changes to the Children's Online Privacy Protection Rule," 19 Apr. 2010, *http://www.ftc.gov/opa/2010/04/coppa.shtm*; Federal Trade Commission, "FTC Seeks Public Comment on Program to Keep Web Site Operators in Compliance With the Children's Online Privacy Protection Rule," 6 Jan. 2010, *http://www.ftc.gov/opa/2010/01/isafe.shtm* (both viewed 26 Apr. 2010).

[19] See, especially, Section 1302980(F) of COPPA.

[20] Federal Trade Commission, "COPPA Rule Review: 2010," *http://www.ftc.gov/privacy/privacyinitiatives/childrens_2010rulereview.html* (viewed 26 Apr. 2010).

consumer data."[21] I also support ensuring that parents have reasonable and effective methods to "review or delete personal information" in their children's online file.

Without question, digital media play a critically important role in the positive development of children and youth, helping them become better educated and providing a foundation for their engagement as citizens.[22] But, there are also risks and dangers online, as many of us are aware. When COPPA was created, one of our concerns was to ensure that the ability to identify, track, and target a child—whether online or off—was mediated through Congressional safeguards mandating parent involvement. And while young people—and adults—today are being continually urged to make more of their personal information available in real-time, including their location, research indicates the few people understand how that information is collected and used. Even young adults, according to a new study released just last week, want to ensure their privacy is secured online. The study, conducted by scholars from UC Berkeley and the Annenberg School for Communication, University of Pennsylvania, found that "large percentages of young adults (those 18–24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy. . . . [Y]oung-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data."[23] As those responsible for the welfare of our children, adults must provide reasonable safeguards for protecting their privacy, especially to help them maneuver through an increasingly complex commercial online data collection marketplace.[24]

Some people suggest that children are now so fully steeped in online technologies that they have become savvy about Internet marketing, and thus need no protections.[25] But while children and youth have embraced new technologies, they cannot be expected to understand the subtle, often covert ways that online marketers are collecting, compiling, and analyzing user data. Nor should youth be held accountable for the public health implications of the new marketing environment. Over the last several years, I have closely examined these developments, helping direct a project examining how digital marketing targets both children and adolescents for food and beverage products linked to the country's youth obesity crisis.[26]

Finally, while passage of COPPA established an important framework for safeguarding our youngest consumers in the digital marketplace, adolescents have no such protections. Neither the online industry nor the Federal Trade Commission has adequately addressed the special privacy issues raised for adolescents. Because of their avid use of new media, adolescents are primary targets for digital marketing.[27]

---

[21] Federal Trade Commission, "Federal Trade Commission Staff Report: Self-Regulatory Principles For Online Behavioral Advertising," Feb. 2009, pp. 21–22, *http://www.ftc.gov/opa/2009/02/behavad.shtm* (viewed 26 Apr. 2010).

[22] MIT Press, "The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning," *http://mitpress.mit.edu/catalog/browse/browse.asp?btype=6&serid=170*; John D. and Catherine T. MacArthur Foundation, "Building the Field of Digital Media and Learning," *http://digitallearning.macfound.org/site/c.enJLKQNlFiG/b.2029199/k.94AC/Latest_News.htm*; Kathryn Montgomery, Barbara Gottlieb-Robles, and Gary O. Larson, "Youth as E-Citizens: Engaging the Digital Generation" (Washington, D.C.: American University, 2004), *http://www.centerforsocialmedia.org/ecitizens/index2.htm* (all viewed 26 Apr. 2010).

[23] Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?" 14 Apr. 2010, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864* (viewed 26 Apr. 2010).

[24] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, "Americans Reject Tailored Advertising and Three Activities that Enable It," 29 Sept. 2009, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214*; Center for Digital Democracy, U.S. PIRG, and World Privacy Forum, "In the Matter of Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others Named Below," Federal Trade Commission filing, 8 Apr. 2010, *http://www.democraticmedia.org/real-time-targeting*; Center for Digital Democracy and U.S. PIRG, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices," Federal Trade Commission filing, 13 Jan. 2009, *http://www.democraticmedia.org/files/FTCmobile_complaint0109.pdf* (all viewed 26 Apr. 2010).

[25] Alice E. Marwick, Diego Murgia Diaz, and John Palfrey, "Youth, Privacy, and Reputation (Literature Review)," Berkman Center Research Publication No. 2010–5, Mar. 2010, p. 10, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163* (viewed 27 Apr. 2010).

[26] Jeff Chester and Kathryn Montgomery, "Interactive Food & Beverage Marketing: Targeting Children and Youth in the Digital Age," Berkeley Media Studies Group, May 2007, *http://www.digitalads.org/documents/digiMarketingFull.pdf* (viewed 26 Apr. 2010).

[27] Kathryn C. Montgomery and Jeff Chester, "Interactive Food and Beverage Marketing: Targeting Adolescents in the Digital Age," Special supplement to *Journal of Adolescent Health* (September 2009): 1–12.

Today's teens are being socialized into this new commercial digital culture, which resonates so strongly with many of their fundamental developmental tasks, such as identity exploration, social interaction, and autonomy.[28] Many teens go online to seek help for their personal problems, to explore their own sexual identities, to find support groups for handling emotional crises in their lives, and sometimes to talk about things they do not feel comfortable or safe discussing with their own parents. Yet, this increased reliance on the Internet subjects them to wholesale data collection and profiling. The unprecedented ability of digital technologies to track and profile individuals across the media landscape, and to engage in "micro" or "nano" targeting, puts these young people at special risk of compromising their privacy. Teens may be internalizing and normalizing these invasive practices that have been so integrally woven into their everyday actions and experiences.

As child advocacy and health groups explained in an April 2008 filing with the FTC, "although adolescents are more sophisticated consumers than young children are, they face their own age-related vulnerabilities regarding privacy." The prevailing formula embraced by industry and endorsed by regulators is rooted in the concept of "notice and choice." It is based on the expectation that consumers will read the privacy policies that online companies post on their websites, and if they don not like the terms, they will "opt out." But most privacy policies offer no real choice; instead the policies are presented as a "take-it-or-leave-it" proposition. Surveys have shown that most adults don't read, nor can they readily understand, the often confusing, technical legalese that characterizes these policies.[29] For underaged youth, these challenges are further complicated. As the children's coalition filing points out, ". . . adolescents, who have less education and are less likely to make the effort to read privacy policies," are "more willing to forgo learning about or protecting against behavioral advertising practices. . . in order to move quickly and freely access websites and socially interact."[30] Social networks have created privacy settings that create a false sense of security for teens. While young people may believe they are protecting their privacy, they remain totally unaware of the nature and extent of data collection, online profiling, and behavioral advertising that are becoming routine in these online communities.

Recent research within the fields of neuroscience, psychology, and marketing has identified key biological and psychosocial attributes of the adolescent experience that may make members of this age group particularly susceptible to interactive marketing and data collection techniques.[31] A number of scholars have challenged the notion that cognitive defenses enable adolescents to resist advertising (particularly in new media) more effectively than younger children.[32] Rather than communicating rational or factual appeals, many digital marketing techniques are forms of "implicit persuasion" that promotes "subtle affective associations," often circumventing a consumer's explicit persuasion knowledge.[33]

In addition to its review of COPPA, the FTC should develop specific recommendations for protecting the privacy of adolescents as part of its broad new initiative on

---

[28] S. Harter, "Processes Underlying the Construction, Maintenance and Enhancement of the Self-concept in Children," *Psychological Perspective on the Self* 3 (1990): 45–78; U. Uhlendorff, "The Concept of Developmental Tasks," *Social Work & Society* 2, n. 1 (2004): 54–63; J. Hill, "Early Adolescence: A Framework," *Journal of Early Adolescence* 3, n. 1 (1983): 1–21; K. Subrahmanyam and P. Greenfield, "Online Communication and Adolescent Relationships," *The Future of Children* 18, n. 1 (2008): 119–146.

[29] Institute for Public Representation (on behalf of the American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, American Psychological Association, Benton Foundation, Campaign for a Commercial Free Childhood, Center for Digital Democracy), filing with the Federal Trade Commission concerning "Online Behavioral Advertising Principles," 11 Apr. 2008, p. 6, *http://www.democraticmedia.org/files/Children's%20Advocacy%20Groups%20%20Behavioral%20Advertising%20Comments%20FINAL.pdf* (viewed 15 June 2008).

[30] Institute for Public Representation FTC filing, pp. 7, 9.

[31] C. Pechmann, L. Levine, S. Loughlin, *et al.*, "Impulsive and Self-conscious: Adolescents' Vulnerability to Advertising and Promotion," *Journal ofPublic Policy & Marketing* 24, n. 2 (2005): 202–221. Frances M. Leslie, Linda J. Levine, Sandra E. Loughlin, and Cornelia Pechmann, "Adolescents' Psychological & Neurobiological Development: Implications for Digital Marketing," June 2009, *http://digitalads.org/documents/Leslie_et_al_NPLAN_BMSG_memo.pdf* (viewed 27 Apr. 2010).

[32] S. Livingstone and E. J. Helsper, "Does Advertising Literacy Mediate the Effects of Advertising on Children? A Critical Examination of Two Linked Research Literatures in Relation to Obesity and Food Choice," *Journal of Communication* 56, n. 3 (2006): 560- 584.

[33] A. Nairn and C. Fine, "Who's Messing with My Mind? The Implications of Dual-process Models for the Ethics of Advertising to Children," *International Journal of Advertising* 27, n. 3 (2008): 447–470.

online privacy. [34] Child advocacy and health groups, for example, have called for an expanded definition of "sensitive data" to include the online activities of all persons under the age of eighteen, as well as a prohibition against "the collection of sensitive information for behavioral advertising purposes." [35]

I hope this committee will send a message to the FTC, as you review the record, that COPPA remains a valuable safeguard for children online, but the rules for implementing it need updating to account for the latest developments in digital marketing. I also urge the Committee to encourage the FTC to protect the privacy of adolescent consumers.

Senator PRYOR. Thank you.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, EPIC AND ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman, members of the Committee. I appreciate the opportunity to be here today.

I'm the Director of EPIC. We're a nonprofit research organization. I also teach privacy law at Georgetown.

I actually wanted to begin by thanking Professor Montgomery for the leadership role she played in helping to ensure passage of the Act. We wrote to the FTC, back in 1995, and asked the Commission to look at the business practices involving the collection and use of personal information on children. And following that letter and the hearings and the subsequent work of the consumer coalition, Congress did, in fact, pass important legislation. And we think that legislation set up the simple principle that, in this new online environment, it was important to protect young people from the exploitation and manipulation of their personal information.

And I think it's obvious that there have been dramatic changes since the time that COPPA has been enacted. And the most obvious change is the emergence of the social network services. Our kids live online, exchanging intimate information with their friends; and that information is then collected and used for marketing purposes. And while their disclosures to their friends appear, to them, to be very transparent and to give them a great deal of control over what they choose to post or not post, what's going on behind the scenes, in terms of the transfer of their data by companies, such as Facebook, to their advertising partners, to their application development partners, and now to the third-party websites that they propose to transfer information about, is much more opaque.

Now, Facebook said earlier—and I think this is true—that, for the most part, they've tried to discourage the use of the service by children under the age of 13 so that they remain compliant with COPPA. But, what they haven't addressed, and I think the critical question now before the Committee, is, How do we deal with the collection and use of this personal information on teenagers, children between the ages of 13, whose data is being collected in this online environment, and then disclosed to marketers and others for purposes completely unrelated to the reasons that they made it available?

---

[34] Federal Trade Commission, "Exploring Privacy: A Roundtable Series," *http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml* (viewed 27 Apr. 2010).

[35] Institute for Public Representation FTC filing, 13.

The problem is more serious, still, because, in this setting, the user has to rely on the privacy policies and the privacy settings that they are presented with. That's essentially the only way, in a self-regulatory environment, you are going to get privacy protection. And what we are seeing, increasingly, is that companies, having collected the data on teenagers, will change the privacy policies, they will change the privacy settings, for the purpose of making this data more easily accessible to business partners for marketing purposes. This is a problem that COPPA never anticipated. And I think it is the single-biggest problem facing children in the online world today. The self-regulatory approach that relies on privacy settings and privacy policies is not working.

And it's also not working, in part, I regret to say, because I don't think the Federal Trade Commission has been as aggressive as it needs to be to go after what are essentially unfair and deceptive trade practices. They do a very good job on the education side, no doubt about it; and they have provided very good materials, to families and teachers and educators and others, about what people need to do to protect the safety of their children online. But, they have not done enough to enforce these unfair and deceptive trade practices. And I think they need to do more.

I want to tell you, briefly, one extraordinary story, a complaint that we filed with the Federal Trade Commission last year that was offering a product, ostensibly, for parental control. It was supposed to protect kids online from, you know, risks and dangers that parents might be worried about. The same company was gathering the data, through this product that they made available, for marketing purposes. And this is how they described their own product, "Every single minute, Pulse is aggregating the Web's social media outlets, such as chat and chat rooms, blogs, forums, instant messaging, and websites, to extract meaningful user-generated content from your target audience: the teens." They're talking to a marketing firm about how they're able to surreptitiously gather information on kids online.

We went to the FTC, and we said to the FTC, "You need to shut down this company." The FTC acknowledged the receipt of our complaint, but never acted on it.

But, the story doesn't end there. When the Department of Defense learned about how this product operated, and they were, at the time, planning to make it available online to military families through their online store, they said, "This poses a risk, a privacy and security risk, to military families, and we will not make it available."

In other words, the Department of Defense, acting on information that anyone who had taken a close look at the product would have quickly recognized was a serious problem, made an appropriate decision.

The FTC, which has the authority and the expertise to police COPPA, never acted.

I think, in both of these areas, the need to update the law so that there are protections for teenagers, those between 13 and 18, from the misuse of the commercial information, and also for the FTC to get much more aggressive on enforcement. Education is not enough

in this area. They have to go after these companies that are not acting appropriately when they collect and use personal data.

Thank you very much.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, EPIC AND ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

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]

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.

---

[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.

[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*.

1The 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 website 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]

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 websites 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 websites,[11] including social network websites,[12] comply with COPPA by implementing privacy safeguards for their young users. Many other websites,[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.

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.

---

[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).
[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.").

On the other, the transfer of user data to application developers and now to websites 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.

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*.

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:

---

[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.*

[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/bonziumg.shtm*.

[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/*.

> Every single minute, Pulse is aggregating the Web's social media outlets such as chat and chat rooms, blogs, forums, instant messaging, and websites 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 e-mail 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:

> 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 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

---

[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.

[24] E-mail 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).

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 RIFD 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.

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/*

---

[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.*

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*

Senator PRYOR. Thank you.
Mr. Szoka.

STATEMENT OF BERIN SZOKA, SENIOR FELLOW AND DIRECTOR, CENTER FOR INTERNET FREEDOM, THE PROGRESS & FREEDOM FOUNDATION

Mr. SZOKA. Mr. Chairman, Mr. Ranking Member, and Committee members, thank you for inviting me here today.

Despite sitting at the kids' table, I am a Senior Fellow at The Progress & Freedom Foundation. So, you can just imagine how young my colleagues must be!

But, I commend the Committee for studying COPPA, and also the Federal Trade Commission, for its review of the COPPA rule, which I think is an important distinction we should keep in mind.

As Ms. Rich explained, for an "Internet junior," as we have referred to it, of sites that are directed to children under 13, COPPA requires sites to either age-verify all users or to limit the functionality of the site to prevent children from making personal information publicly available, including the sharing of user-generated content.

COPPA imposes the same requirement on general audience sites when they have actual knowledge that they are collecting information from a user under 13 or, again, enabling them to share information.

Because of this forced separation and the costs of age verification, COPPA may well have unintentionally limited the choice and competition in the marketplace for children's content by driving consolidation in that marketplace.

On the other hand, COPPA has been reasonably successful in fulfilling Congress's original goal of enhancing parental involvement to protect children's online privacy and safety.

Whatever this tradeoff, I am here today to caution against expanding COPPA beyond its original, limited purpose. COPPA's unique value lies in its flexibility, its subtlety, and its intentional narrowness. And my concern here is not just about innovation, but also about free speech.

COPPA is flexible, because it potentially applies the—to the entire Internet, regardless of the access device used, including services scarcely imaginable in 1998.

COPPA is subtle, because it requires verifiable parental consent, not only if site and service operators gather personal information

from kids for their own use, but also if they enable children to make that information publicly available online.

Even more subtle, however, is COPPA's creative solution to the thorny problem of age verification. And, in a nutshell, I would say that 13 is just right. Unlike the similarly named Child Online Protection Act, or COPA, COPPA requires age verification of users on sites clearly directed at children only—and, again, where they have actual knowledge; whereas, COPA required age verification of all users for any site offering content deemed harmful to minors.

Back in 1998, Congress considered, but wisely chose not, to apply COPPA to adolescents. Unfortunately, recent efforts to expand COPPA have put online privacy, child safety, free speech, and anonymity on a collision course. Several states have proposed what we, at PFF, have called "COPPA 2.0 laws," extending COPPA to adolescents under 17 or 18. But, once the age threshold rises above 13, it becomes increasingly difficult to distinguish sites directed at children below the threshold from general audience sites. With this seemingly small change, COPPA would essentially converge with COPA. COPPA would extend beyond a discreet Internet junior to require age verification for sites used by many adults. And indeed, other states have proposed simply extending COPPA to all social networking sites.

But, requiring adults and even older teens to prove their age by identifying themselves constitutes a prior restraint on anonymous or pseudo anonymous communications. And this would raise the same First Amendment concerns that caused the courts to strike down COPA.

Ironically, broader age verification mandates would actually reduce online privacy by requiring more information to be collected, both from adolescents and from adults, which would include credit card information. While COPPA's safe harbor is playing a valuable part in administering self-regulation under COPPA, government shouldn't put them in the awkward position of becoming repositories for huge troves of personal information in the name of protecting privacy.

Nor would COPPA expansion make adolescents safer online. Some have argued that age-verification mandates could protect children by allowing sites to create safe spaces that exclude predators. Unfortunately, the reality is that technology for reliable age verification simply does not exist. Even the FTC has made it clear that it doesn't consider COPPA's verifiable parental consent methods, such as the use of a credit card, as equivalent to strict age verification.

COPPA could—expansion could also undermine the viability of many online sites and services. As you've heard here today, some consider the real marketers—excuse me—marketers to be the real predators, even though advertising is what we have called "the great hidden benefactor" that funds the overwhelming majority of free online content and services. COPPA already applies to the collection of personal information that could potentially allow the contacting of children under 13, and the Network Advertising Initiative already requires verifiable parental consent for behavioral advertising to children under 13. But, if COPPA were expanded to require general audience sites funded by tailored advertising to age-

verify all users, it would devolve into the unconstitutional approach found in COPPA.

Importantly, COPPA expansion would also raise costs for smaller or new sites and services geared toward minors. And, in turn, this could discourage innovation, limit choice, and raise prices for consumers, and, as I mentioned before, also potentially restrict speech.

But, ultimately, concerns about tailored advertising may be less about privacy or safety than what about—advertising scholar Jack Calfee, of the American Enterprise Institute, has called "the fear of persuasion," the idea that advertising is inherently manipulative, and grows only more so with increased relevance. As he has noted, by 10 or so, children have a full understanding of the purpose of advertising, and, equally important, an active suspicion of what advertisers say. If government has a role in—to play in addressing concerns about tailored marketing, it lies in educating kids about advertising, to help them become smarter consumers.

Last week, the FTC launched just such an education campaign, with its AdMongo tutorial website. The FTC excels in consumer education, and should be encouraged in these efforts as a less restrictive alternative to regulation.

Finally, briefly, I want to caution that H.R. 4173, passed by the House in the fall, would give the FTC the capability, even if it didn't intend to do so today, to unilaterally change COPPA, including its age range. And I would simply suggest that such changes should be made by Congress, and not the FTC. If Congress wants to help the FTC implement COPPA, it should consider additional funding for education, and indeed for enforcement.

Thank you for inviting me to testify.

[The prepared statement of Mr. Szoka follows:]

PREPARED STATEMENT OF BERIN SZOKA, SENIOR FELLOW AND DIRECTOR, CENTER FOR INTERNET FREEDOM, THE PROGRESS & FREEDOM FOUNDATION

Mr. Chairman and Committee members, thank you for inviting me here today. My name is Berin Szoka.[1] I'm a Senior Fellow at The Progress & Freedom Foundation (PFF). PFF is a market-oriented think tank and 501(c)(3) non-profit founded in 1993 that studies the digital revolution and its implications for public policy. PFF's mission is to educate policymakers, opinion leaders, and the public about issues associated with technological change, based on a philosophy of limited government, free markets, and individual sovereignty.

I commend this committee for studying the Children's Online Privacy Protection Act or COPPA, and the FTC for its upcoming COPPA Review and Roundtable.[2] My colleague Adam Thierer, PFF's President, has been actively engaged in debates about online child safety and privacy since joining PFF in 2005, and is the author of *Parental Controls & Online Child Protection: Survey of Tools & Methods,* a regularly updated compendium now in its fourth edition and available for free online.[3] The constant theme in PFF's work in this area has been to emphasize the tools and methods available to parents to control their children's use of media, including the Internet and to the central role played by education efforts in helping both parents and children make smarter choices. We also highlight enforcement of existing laws as an additional "less restrictive" alternative to new regulation, and attempt to

[1] The views expressed here are his own, and not necessarily the views of the PFF board, other fellows or staff.

[2] Federal Trade Commission, *Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Rule*, April 5, 2010, *http://www.ftc.gov/os/2010/03/100324coppa.pdf*; *see also* COPPA Rule Review Roundtable, *http://www.ftc.gov/bcp/workshops/coppa/index.shtml*.

[3] Adam Thierer, *Parental Controls & Online Child Protection: Survey of Tools & Methods*, Version 4.0, Fall 2008, *www.pff.org/parentalcontrols/index.html*.

highlight the trade-offs involved in imposing new regulation of online communications.

In May 2009, Adam and I published a 35-page paper entitled *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, providing an overview of COPPA, how it works, its costs and benefits, and explaining the dangers inherent in several then-pending efforts to expand COPPA by expanding the law to cover adolescents or all social networking sites.[4] We identified a number of legal, technical, and other practical problems with such proposals in that they would:

- Burden the free speech rights of adults by imposing age verification mandates on many sites used by adults, thus restricting anonymous speech and essentially converging—in terms of practical consequences—with the unconstitutional Children's Online Protection Act (COPA),[5] another 1998 law sometimes confused with COPPA;
- Burden the free speech rights of adolescents to speak freely on—or gather information from—legal and socially beneficial websites;
- Hamper routine and socially beneficial communication between adolescents and adults;
- Reduce, rather than enhance, the privacy of adolescents, parents and other adults because of the massive volume of personal information that would have to be collected about users for authentication purposes (likely including credit card data);
- Would likely be the subject of massive fraud or evasion since it is not always possible to definitively verify the parent-child relationship, or because the system could be "gamed" in other ways by determined adolescents;
- Do nothing to prevent offshore sites and services from operating outside these rules;
- Present major practical challenges for law enforcement officials in the face of such evasion by both domestic users and offshore sites;
- Could destroy opportunities for new or smaller website operators to break into the market and offer competing services and innovations, thus contributing to consolidation of online content and services by erecting barriers to entry; and
- Violate the Commerce Clause of the U.S. Constitution if enacted by states, since Internet activity clearly represents interstate commerce that states have no authority to regulate.

This testimony summarizes the key aspects of that paper, which I attach below for the Committee's convenience, but also provides additional context on subsequent developments and related issues. Subsequently, I filed written testimony with the Maine Legislature regarding proposals in Maine, including a law enacted over the summer but never enforced by the state attorney general, to apply the COPPA framework to the collection of health-related information from adolescents.[6] We also look forward filing comments in the FTC's upcoming COPPA Review.

COPPA can best be summarized as follows: For an "Internet Jr." of sites "directed at" children under 13, COPPA requires sites either to age-verify all users or limit functionality to prevent children from making personal information "publicly available"—including the sharing of user-generated content. COPPA imposes the same requirement on general audience sites when they have actual knowledge a user is under 13.

The Costs of COPPA

Because of this forced separation and the costs of age verification, COPPA may well have unintentionally limited choice and competition by driving increased consolidation in the marketplace for child-oriented sites and services online and discouraging new entry by smaller "mom-and-pop" sites that could cater to children. As early as 2001, even some Congressmen recognized this "unintended consequence"

---

[4] Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Progress on Point 16.11, May 2009, *http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf*.

[5] 47 U.S.C. § 231. While COPPA governs sites "directed at" children, COPA would have required age verification for content deemed "harmful to minors." COPA has been struck down on First Amendment grounds.

[6] Berin Szoka, *Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677*, March 4, 2010, *www.pff.org/issues-pubs/filings/2010/2010-03-04-Maine_Law_Testimony.pdf*.

of COPPA in Congressional hearings on privacy.[7] There are significant costs associated with the verifiable parental consent methods used to comply with COPPA. Of course, it could be the case that there are other reasons that there are relatively few sites catering exclusively to children. But this is a question worth considering, and the FTC deserves credit for beginning its COPPA review with this question.[8] As noted by Parry Aftab, Executive Director of the children's advocacy group Wired Safety, "COPPA wasn't responsible for the demise of these sites, but when combined with the other factors [it] tipped the balance."[9] She concludes, appropriately:

> It is crucial that at this tentative stage for the kids Internet industry we don't do anything to make its survival more difficult. We should be looking at easy to encourage safer communities for preteens and innovations to help create fun, entertaining and educational content for kids online.[10]

The Success of COPPA

On the other hand, COPPA has been reasonably successful in fulfilling Congress's original goals, as expressed by the law's Congressional sponsors:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[11]

Thus, as its name implies, COPPA is first and foremost about protecting the privacy of children. COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools . . . for becoming involved in and overseeing their children's interactions online."[12] However admirable, "protect[ing] the safety of children" is merely an *indirect* goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's *direct* goal). The FTC declares that COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[13]

Indeed, COPPA may succeed in achieving its original purpose of enhancing parental involvement, but strict age verification mandates intended to go beyond COPPA will ultimately fail because kids will simply lie to circumvent age verification requirements. As Microsoft researcher Danah Boyd has put it, "COPPA did not stop most children from creating accounts, but it did teach children and their parents an important lesson: Lying is the path to access."[14] Even though "there is no perfect solution" and it is not possible to completely "stop a child from lying and putting themselves at risk," Denise Tayloe of Privo, one of the four FTC-approved providers of COPPA safe harbor age verification services, believes that COPPA "provides a platform to educate parents and kids about privacy."[15]

---

[7] Rep. Billy Tauzin (R–LA) noted that COPPA "has now forced companies to discontinue a number of products targeted toward children" and asked "If we end up forcing private companies and nonprofits to eliminate beneficial products such as crime prevention material, have we done a good thing? If teen-friendly sites, those that totally respect the privacy of the users stop offering e-mail services to children, is that a good thing? *An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing of the House Committee On Energy and Commerce, 107th* Cong. 6 (April 3, 2001) (statement of Rep. Tauzin.), available at *http://republicans.energycommerce.house.gov/107/action/107–22.pdf.*

[8] Federal Trade Commission, *Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Rule*, at 2 April 5, 2010, *http://www.ftc.gov/os/2010/03/100324coppa.pdf.*

[9] *Comments of Parry Aftab, Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children* at 3, June 27, 2005, *www.ftc.gov/os/comments/COPPArulereview/516296–00021.pdf.*

[10] *Id.*

[11] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[12] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 28, Feb. 2007, *www.ftc.gov/reports/coppa/07COPPA__Report__to__Congress.pdf.*

[13] *Id.*

[14] Danah Michele Boyd, *Taken Out of Context American Teen Sociality in Networked Publics,* at 151 Fall 2008, *www.danah.org/papers/TakenOutOfContext.pdf.*

[15] E-mail from Denise Tayloe to Adam Thierer (Mar. 15, 2007) (copy on file with author).

Especially given this practical limitation and whatever the trade-offs involved in COPPA, I'm here today to caution against expanding COPPA beyond its original, limited purpose. COPPA's unique value lies in its flexibility, subtlety, and intentional narrowness.

COPPA is Flexible Enough to Cover a Rapidly Changing Landscape

COPPA is flexible because it potentially applies to the entire Internet regardless of the access device used—including services scarcely imaginable in 1998. Specifically, COPPA applies to any "operator," which the statute defines to mean:

> 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.[16]

COPPA defines the key term "Internet" broadly to mean:

> collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide 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.[17]

In interpreting its COPPA Rule, the FTC has said:

> The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.[18]

Because nearly all communications platforms have converged on the "Internet," thus defined, COPPA would reach a wide variety of services and media not commonly thought of as belonging to the "Internet." For example, if a video game console is networked through the Internet to allow users to play games with each other, COPPA would apply to potential sharing of personal information. To this extent, the FTC ought not need new statutory authority from Congress.

COPPA's Subtlety Lies in its Narrowness

COPPA is subtle because it requires "verifiable parental consent" not only if site and service operators gather personal information from kids for their own use, but also if sites enable children to make personal information "publicly available" online. Even more subtle is COPPA's creative solution to the thorny problem of age verification. Unlike the similarly-named Child Online Protection Act of 1998 (COPA, pronounced *"koh-pah"* instead of *"kah-pah"*),[19] COPPA only requires age verification of users onsites clearly directed at children, whereas COPA required it for any site offering content deemed "harmful to minors."

Efforts to Expand COPPA Raise Serious First Amendment Concerns

Back in 1998, Congress wisely chose not to apply COPPA to adolescents. Unfortunately, recent efforts to expand COPPA have put online privacy, child safety, free speech and anonymity on a collision course. Several states have proposed what we at PFF have called "COPPA 2.0" laws, extending COPPA to adolescents up to 17 or 18. But once the age threshold rises above 13, it becomes increasingly difficult to distinguish sites "directed at" children below the threshold from general audience sites. With this seemingly small change, COPPA would essentially converge with COPA: COPPA would extend beyond a discrete "Internet, Jr." to require age verification for sites used by many adults—and, indeed, other states have proposed simply extending COPPA to all social networking sites. But requiring adults and even older teens to prove their age by identifying themselves constitutes a prior restraint on anonymous or pseudonymous communication. This raises the same First Amendment concerns that caused the courts to strike down COPA.

After a decade-long court battle over COPA's constitutionality, the U.S. Supreme Court in January 2009 rejected the government's latest request to revive the law,

---

[16] 15 U.S.C. § 6501(2).

[17] 15 U.S.C. § 6501(6).

[18] Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, Question 6 ("What types of online transmissions does COPPA apply to?"), *www.ftc.gov/privacy/coppafaqs.shtm*.

[19] 47 U.S.C. § 231.

meaning it is likely dead.[20] Three of the key reasons the courts struck down COPA would also apply to COPPA 2.0 proposals:

- *Anonymous Speech Rights of Adults*. COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial."[21] The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication.[22] By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves *more* protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz.*, pornography), COPPA 2.0 would burden access to material by adults as well as minors not because that material is harmful or obscene but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications about political nature, which deserved the highest degree of First Amendment protection.
- *Speech Rights of Site Operators.* The necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is that COPPA 2.0 proposals would, like COPA, necessarily reduce the audience size of websites subject to age verification mandates. Furthermore, such mandates would encourage websites to self-censor themselves to avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate—or to legal liability if they fail to implement age verification. The substantial cost of age verification could significantly impact, if not make impossible, sites that allow sharing of personal information, including user-generated content, because such sites generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[23]
- *Less Restrictive Alternatives to Regulation.* The Third Circuit drew on the Supreme Court's 2004 decision striking down COPA on the grounds that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[24] Similarly, parental control software already empowers parents to restrict their kids' access to sites that "collect" personal information. It's particularly easy for parents to restrict access to the leading social networking sites that seem to be driving so much of the push for COPPA 2.0.

COPPA Expansion Would Undermine Privacy

Ironically, broad age verification mandates would *reduce* online privacy by requiring *more* information to be collected from both adolescents and adults, including credit card information, in order to verify age and the parent/child relationship (in the admittedly imperfect fashions prescribed by COPPA's "Sliding Scale"). While COPPA's safe harbor administrators play a valuable role in administering self-regulation under COPPA,[25] government shouldn't put them in the awkward position of

---

[20] *See* Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA*, PFF Blog, Jan. 21, 2009, *http://blog.pff.org/archives/2009/01/closing_the_boo.html. See also* Alex Harris, *Child Online Protection Act Still Unconstitutional, http://cyberlaw.stanford.edu/packet/200811/child-online-protection-act-still-unconstitutional.*

[21] *American Civil Liberties Union* v. *Ashcroft*, 322 F.3d 240, 259 (3d Cir. 2003).

[22] *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also Talley* v. *California*, 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

[23] *See ACLU III*, 534 F.3d at 196–97 (citing *ACLU* v. *Gonzales*, 478 F. Supp. 2d 775, 804). The Court held that websites "face significant costs to implement [COPA's age verification mandates] and will suffer the loss of legitimate visitors once they do so." *Id.* at 197.

[24] *Id.* at 198 (quoting *ACLU* v. *Mukasey*, 534 F.3d 181, 198 (2008)).

[25] The four safe harbor programs are administered by the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo. *See* Federal Trade Commission, *Safe Harbor Program*, *www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.*

becoming repositories for huge troves of personal information in the name of protecting privacy.

COPPA Expansion Would Not Enhance Child Safety

Some have argued that age verification mandates could protect children by allowing sites to create "safe spaces" that exclude predators. Unfortunately, the reality is that the technology for reliable age verification simply doesn't exist.

Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of websites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[26] Few public data bases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that *do* exist about their children (*e.g.,* birth certificates, Social Security numbers, school records) to become more easily accessible.[27] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[28] Even the FTC has made clear that it doesn't consider COPPA's "sliding scale" of verifiable parental consent methods—use of a credit card, print-and-fax forms, follow-up phone calls and e-mails, and using encryption certificates[29]—as equivalent to strict age verification.[30]

Fears of Advertising Should Not Drive COPPA Expansion

COPPA expansion could also undermine the viability of many online sites and services. Some consider marketers the "real predators"—even though advertising is the great "Hidden Benefactor"[31] that funds the overwhelming majority of "free" Internet content and services. COPPA already applies to the collection of information that could potentially allow the contacting of a child under 13. The Network Advertising Initiative already requires verifiable parental consent for behavioral advertising to children under 13. But if COPPA were expanded to require general audience sites funded by tailored advertising to age-verify all users, it would devolve into the unconstitutional approach found in COPA. Importantly, COPPA expansion would also raise costs for smaller or new sites and services geared toward minors. This could discourage new innovation, limit choice, and raise prices for consumers.[32]

Ultimately, concerns about tailored advertising may be less about privacy than about what advertising scholar Jack Calfee has dubbed the "Fear of Persuasion"—the idea that advertising is inherently manipulative and only grows more so with increased relevance. But as Calfee notes, "by the age 10 or so, children develop a full understanding of the purpose of advertising and equally important, an active suspicion of what advertisers say."[33] If government has a role to play in addressing concerns about tailored marketing, it lies in educating kids about advertising to help them become smarter consumers. Last week, the FTC launched just such an edu-

---

[26] *Gonzales*, 478 F. Supp. 2d at 806.

[27] *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion,* PFF Blog, Sept. *25, 2008, http://blog.pff.org/archives/2008/09/age_verificatio_1.html.*

[28] Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.*

[29] 16 C.F.R. § 312.5(b)(2).

[30] In a February 2007 report to Congress about the status of the law and its enforcement, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online." Federal Trade Commission, Implementing the Children's Online Privacy Protection Act: A Report to Congress at 1, Feb. 2007, *www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.* In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof." *Id.* at 13. The FTC attempts to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms." *Id.* at 12.

[31] Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates & Benefits Consumers*, Progress on Point 6.5, Feb. 2010, *www.pff.org/issues-pubs/ps/2010/pdf/ps6.5-the-hiddenbenefactor.pdf.*

[32] In 2005, the FTC has cited an estimate of $45/child as the cost of obtaining verifiable parental consent for child-oriented sites to comply with COPPA. *See Comments of Parry Aftab, Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children* at 2, June 27, 2005, *www.ftc.gov/os/comments/COPPArulereview/516296–00021.pdf.*

[33] Jack Calfee, American Enterprise Institute, *Fear of Persuasion: A New Perspective on Advertising and Regulation*, 59 (1997).

cation campaign with its AdMongo tutorial website (*www.admongo.gov*).[34] The FTC excels in consumer education, and should be encouraged in these efforts as a less restrictive alternative to regulation. Other excellent examples of FTC education efforts include:

OnGuardOnline.gov (tips on online security, fraud avoidance and privacy);

NetCetera: Chatting With Kids About Being Online (*www.onguardonline.gov/topics/netcetera.aspx*); and

You Are Here: Where Kids Learn to be Smarter Consumers (*ftc.gov/youarehere/*).

Opening the Door to COPPA Expansion through FTC Overhaul via Financial Reform

Finally, financial reform legislation recently passed by the House would give the FTC sweeping new rulemaking powers, and could allow the FTC to unilaterally change COPPA, including its age range. Specifically, H.R. 4173 would give the FTC normal rulemaking authority under the Administrative Procedures Act, replacing the special rulemaking procedures crafted by Congress with the 1975 Magnuson-Moss Act, and strengthened through additional procedural safeguards in 1980, to ensure that the agency did not rush into preemptive regulation without carefully weighing the costs and benefits of government intervention.[35]

Such decisions should be made by Congress, not the FTC. If Congress wants to help the FTC implement COPPA, it should consider additional funding for education and enforcement. These, in conjunction with empowerment of parents and kids to manage their own privacy and other online preferences, offer a better approach to addressing concerns about online child privacy and safety than increased regulation.

Thank you again for inviting me to testify.

Related PFF Publications

- *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Berin Szoka & Adam Thierer, Progress on Point 16.11, May 2009.
- *Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677,* Berin Szoka, March 4, 2010.
- *Parental Controls & Online Child Protection: A Survey of Tools & Methods*, Adam Thierer, Special Report, Version 4.0, Fall 2008.
- *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, Adam Thierer, Progress on Point 16.13, July 8, 2009.
- *The Perils of Mandatory Parental Controls and Restrictive Defaults*, Adam Thierer, Progress on Point 15.4, April 11, 2008.
- *Written Testimony before House Committee on the Judiciary on Cyber Bullying and other Online Safety Issues for Children*, Berin Szoka & Adam Thierer, September 30, 2009.
- *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments of Berin Szoka to FTC Exploring Privacy Roundtable, Nov. 2009.
- *Privacy Polls v. Real-World Trade-Offs*, Berin Szoka, Progress Snapshot 5.10, Oct. 2009.
- *Online Advertising & User Privacy: Principles to Guide the Debate*, Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.
- *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.
- *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Berin Szoka, Progress Snapshot 6.7, March 2010.

---

[34] *Federal Trade Commission to Launch Advertising Literacy Campaign National Program Gives 'Tweens' Ages 8 to 12 Skills to Recognize, Understand Advertising*, April 26, 2010, *www.ftc.gov/opa/2010/04/admongo.shtm*.

[35] *See generally,* Berin Szoka, *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Progress Snapshot 6.7, March 2010, *www.pff.org/issues-pubs/ps/2010/pdf/ps6.7-FTC_on_steroids.pdf*.

The Progress & Freedom Foundation—Progress on Point—Volume 16, Issue 11—May 2009

COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech

by Berin Szoka & Adam Thierer

Executive Summary

Online privacy, child safety, free speech and anonymity are on a collision course. The 1998 Children's Online Privacy Protection Act (COPPA) already mandates certain online privacy protections for children under 13, but many advocate expanding online privacy protections for both adolescents and adults. Furthermore, efforts continue at both the Federal and state levels to institute new regulations, such as age verification mandates, aimed at ensuring the safety of children online. There is an inherent tension between these objectives: Attempts to achieve perfectly "safe" online environments will likely require the surrender of some privacy and speech rights, including the right to speak anonymously.

These tensions are coming to a head with state-based efforts to expand COPPA, which requires "verifiable parental consent" before certain sites or services may collect, or enable the sharing of, personal information from children under the age of 13. Several proposed state laws would extend COPPA's parental-consent framework to cover all adolescents under 18. This seemingly small change would require age verification of not only adolescents and their parents, but—for the first time—large numbers of adults, thus raising grave First Amendment concerns. Such broad age verification mandates would, ironically, *reduce* online privacy by requiring *more* information to be collected from both adolescents and adults for age verification purposes, while doing little to make adolescents safer. In practical terms, the increased scale of "COPPA 2.0" efforts would present significant implementation and enforcement challenges. Finally, state-level COPPA 2.0 proposals would likely conflict with the Constitution's Commerce Clause.

Despite these profound problems, COPPA expansion has great rhetorical appeal and seems likely to be at the heart of future child safety debates—especially efforts to require mandatory age verification. There are, however, many better ways to protect children online than by expanding COPPA beyond its original, limited purpose.

I. Introduction

When the debate about social networking safety first heated up a few years ago, some state attorneys general (AGs) and vendors of age verification services implied that the technology existed—or could be easily developed—to verify the age of any minor who sought access to an interactive website.[1] Federal law currently requires—via the Children's Online Privacy Protection Act (COPPA) of 1998[2]—that child-oriented website operators or service providers "Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children [under 13]."[3] But advocates of age verification mandates have argued that online child safety would be improved if websites—particularly "social networking sites" like MySpace, Facebook and Bebo—were required to do more: screen users by age and to limit or ban access by those over, or under, a certain age.

Today, however, the practical limitations and dangers of age verification mandates have become more widely recognized. Few continue to argue for directly mandating verification of the age of minors online—or that such verification, in its strictest sense, is even technically feasible. Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of websites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[4] Few public data bases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that *do* exist about their children (*e.g.,* birth certificates, Social Security

---

[1] *See, e.g.,* Emily Steel & Julia Angwin, *MySpace Receives More Pressure to Limit Children's Access to Site, Wall Street Journal,* June 23, 2006, *http://online.wsj.com/public/article/SB115102268445288250-YRxkt0rTsyyf1QiQf2EPBYSf7iU_20070624.html*.

[2] 15 U.S.C. §§ 6501–6506.

[3] *See* 16 C.F.R. § 312.5. *See infra* at 6 and note 25 for a discussion of COPPA's other requirements, particularly that COPPA applies if a website has "actual knowledge" that it is collecting information from a child even if the website is not "directed at" children.

[4] *ACLU* v. *Gonzales,* 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) [hereinafter Gonzales]; *see infra* at 28.

numbers, school records) to become more easily accessible.[5] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[6]

There are a host of other concerns about age verification mandates.[7] Some of these concerns were summarized in a recent report produced by the Internet Safety Technical Task Force, a blue ribbon task force assembled in 2008 by state AGs to study this issue:

> Age verification and identity authentication technologies are appealing in concept but *challenged in terms of effectiveness.* Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.[8]

With opposition to strict age verification mandates growing, some regulatory advocates now seek to institute such mandates through the back door of "parental consent" mandates in the model of COPPA. Such "COPPA 2.0" legislation has been introduced at the state level that would extend the COPPA parental-consent framework to cover all minors between the ages of 13 and 17 inclusive ("adolescents"). Some of these bills would also broaden the range of sites covered, increase the amount of information required to be collected to achieve "verifiable parental consent" or impose other mandates such as parental access.

Two such bills were introduced in 2007, in North Carolina (with the support of that state's Attorney General Roy Cooper)[9] and Georgia.[10] While these bills were never passed, a similar bill is currently pending in Illinois.[11] Because the scope of such bills would reach all "social networking sites" that offered certain functionality (*e.g.,* user profiles), rather only those sites directed at a particular age bracket (as under COPPA),[12] they would extend age verification mandates far beyond sites that might be considered "adolescent-oriented." Another bill is currently pending in New Jersey; like COPPA, this bill would reach only sites directed at adolescents, but it might reach a broader range of sites, because its scope is not limited specifically to

---

[5] *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion,* PFF Blog, Sept. 25, 2008, *http://blog.pff.org/archives/2008/09/age_verificatio_1.html.*

[6] Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.*

[7] For a fuller exploration of these issues, *see* Adam Thierer, The Progress & Freedom Foundation, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,* Progress on Point No. 14.5, Mar. 2007; Adam Thierer, The Progress & Freedom Foundation, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General,* Jan. 14, 2008, *www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf;* Nancy Willard, *Why Age and Identity Verification Will Not Work—And is a Really Bad Idea,* Jan. 26, 2009, *www.csriu.org/PDFs/digitalidnot.pdf; Jeff Schmidt, Online Child Safety: A Security Professional's Take,* The Guardian, Spring 2007, *www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.*

[8] Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States,* Dec. 31, 2008, at 10, *http://cyber.law.harvard.edu/pubrelease/isttf* [hereinafter ISTTF Final Report]. Full disclosure: Adam Thierer was a member of this task force.

[9] S.B. 132, 2007 Gen. Assem., Reg. Sess. § 8 (N.C. 2007), available at *www.ncga.state.nc.us/Sessions/2007/Bills/Senate/HTML/S132v3.html; see also* Roy Cooper, *Protecting Children from Sexual Predators: SB 132,* July 24, 2007, *www.ncdoj.com/DocumentStreamerClient?directory=WhatsNew/&file=S132%20summary%20final.pdf; see also* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Showdown in North Carolina,* PFF Blog, July 26, 2007, *http://blog.pff.org/archives/2007/07/age_verificatio.html.*

[10] S.B. 59, Gen. Assem., 2007–2008 Leg. Sess. (Ga. 2007), available at *www.legis.ga.gov/legis/2007_08/fulltext/sb59.htm.*

[11] H.B. 1312, 96th Gen. Assem., Synopsis as Introduced (Il. 2007) [hereinafter SNWARA], available at *www.ilga.gov/legislation/billstatus.asp?DocNum=1312&GAID=10&GA=96&DocTypeID=HB&LegID=43038&SessionID=76.*

[12] *See infra* note 22 and associated text (noting that that COPPA also applies in cases of "actual knowledge," even if a site is not "directed at" children); *see also infra* Section V.A. (discussing the meaning of "directed at").

"social networking" functionality.[13] The introduction of these bills makes it clear that future online identity verification debates will be increasingly tied up with efforts to expand the COPPA framework. These mandates will likely arrive in the form of state-level expansions of, or Federal amendments to, COPPA, or such proposals will at least cite COPPA's regulatory framework as precedent. Yet COPPA 2.0 advocates seem to forget that, back in 1998, Congress considered, but ultimately rejected, a requirement in the original version of COPPA that operators make "reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[14] This requirement would have been significantly less burdensome than the COPPA 2.0 approaches advanced today, but it was stricken from the final version of COPPA after likely constitutional and practical problems were identified.[15]

Today's COPPA 2.0 bills are fraught with even greater legal, technical, and other practical problems in that they would:

- Burden the free speech rights of adults by imposing age verification mandates on many sites used by adults, thus restricting anonymous speech and essentially converging—in terms of practical consequences—with the unconstitutional Children's Online Protection Act (COPA),[16] another 1998 law sometimes confused with COPPA;
- Burden the free speech rights of adolescents to speak freely on—or gather information from—legal and socially beneficial websites;
- Hamper routine and socially beneficial communication between adolescents and adults;
- Reduce, rather than enhance, the privacy of adolescents, parents and other adults because of the massive volume of personal information that would have to be collected about users for authentication purposes (likely including credit card data);
- Would likely be the subject of massive fraud or evasion since it is not always possible to definitively verify the parent-child relationship, or because the system could be "gamed" in other ways by determined adolescents;
- Do nothing to prevent offshore sites and services from operating outside these rules;
- Present major practical challenges for law enforcement officials in the face of such evasion by both domestic users and offshore sites;
- Could destroy opportunities for new or smaller website operators to break into the market and offer competing services and innovations, thus contributing to consolidation of online content and services by erecting barriers to entry; and
- Violate the Commerce Clause of the U.S. Constitution, since Internet activity clearly represents interstate commerce that states have no authority to regulate.

There are better approaches to protect adolescents that do not implicate the serious legal and societal issues raised by COPPA 2.0 efforts.[17] Attempts to expand COPPA to cover adolescents are thus unnecessary and misguided and should be rejected at both the state and Federal levels.

The FTC should consider carefully the limitations of COPPA and the pitfalls of COPPA 2.0 as the agency prepares to begin an expedited review of COPPA (five years ahead of schedule).[18]

---

[13] A.B. 108, Gen. Assem., 213th Leg. Sess. (N.J. 2008) [hereinafter AOPPA], available at *www.njleg.state.nj.us/2008/Bills/A0500/108_11.HTM.*

[14] Children's Online Privacy Protection Act, S. 2326, 105th Cong. §3(a)(2)(iii) (1998).

[15] Testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology, before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Communications, Sept. 23, 1998, available at *www.cdt.org/testimony/980923mulligan.shtml [hereinafter Mulligan Testimony*].

[16] 47 U.S.C. § 231. While COPPA governs sites "directed at" children, COPA would have required age verification for content deemed "harmful to minors." COPA has been struck down on First Amendment grounds. *See infra* at Section VI.

[17] *See generally* Adam Thierer, The Progress & Freedom Foundation, *Parental Controls and Online Child Protection: A Survey of Tools and Methods,* Special Report, Version 3.1, Fall 2008, *www.pff.org/parentalcontrols/index.html* (cataloguing the tools and methods available to parents to control their kids' Internet use).

[18] Howard Buskirk & Yu-Ting Wang, *FTC to Expedite Review of Children's Online Privacy Protection Rule,* Communications Daily, April 23, 2009, at 5–7.

Before examining in greater detail the problems posed by COPPA 2.0 proposals (Sections IV-VIII), we review how COPPA 1.0 currently works (Section II) and what it achieves (Section III).

II. Current Implementation of COPPA

Terminology

"Adult"—Anyone 18 and over

"Minor"—Anyone under 18

"Child"—Anyone under 13

"Adolescent"—Anyone 13 or over but less than 18

"Kid"—Because of the specific meaning of "child" under COPPA, we have used "kid" instead of "child" when discussing interaction with parents and as a colloquial catch-all where appropriate.

"PI-collecting site"—Any site that collects what COPPA considers "personal information," which includes contact information.

"Social networking site"—A generic term for a PI-collecting site focused on user profiles and connections among users. Some legislative proposals use this term to refer to sites with specific functionality.

COPPA generally requires that commercial operators of websites and services obtain "verifiable parental consent" before collecting, disclosing or using "personal information" (*e.g.,* name, contact information)[19] about children under 13[20] if either (i) their website or service (or "portion thereof") is "directed at children"[21] or (ii) they have actual knowledge that they are collecting personal information from a child.[22] Even if sites and services that collect personal information ("PI-collecting sites"[23]) are not "directed at" children, they must still have such a process in place to deal with cases in which a child has disclosed that they are under 13. The FTC has defined COPPA's scope so broadly that it could apply even to virtual worlds and multiplayer online games (*e.g.,* Second Life, World of Warcraft).[24] COPPA also requires certain notices about information collection, parental access to information collected about children, reasonable data security procedures, and restrictions on the collection of personal information through games and prizes.[25]

---

[19] The FTC has defined "personal information" to include:

(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.

16 C.F.R. § 312.2.

[20] The word "child" is sometimes used interchangeably with the legal term "minor" (someone under 18) in Federal law. *See, e.g.,* 18 U.S.C. § 2256(1) (defining "minor" as "any person under the age of eighteen years") and 18 U.S.C. § 2256(8) (defining "child pornography" as "any visual depiction . . . of sexually explicit conduct [involving a minor]"). In common speech, the term "child" is often used to mean "a son or daughter of any age." *Dictionary.com,* "child," Merriam-Webster's Dictionary of Law, *dictionary.reference.com/browse/child.* By contrast, COPPA defines "child" as a subset of "minor." COPPA 2.0 bills would apply to older minors not currently subject to COPPA, generally referred to as "adolescents."

[21] 16 C.F.R. § 312.2 (definition of "website or online service directed to children"); *see infra* at 22–24 (discussing the FTC's criteria for deciding what constitutes a site "directed to" children).

[22] *See* 16 C.F.R. § 312.3; *see also* 16 C.F.R. § 312.2 (definition of "website or online service directed to children").

[23] We use the term "PI-collecting sites" to refer to both sites and services only for lack of a clearer catch-all.

[24] As the FTC has explained:

COPPA applies to personal information collected online by websites and online services located on the Internet. The Rule defines "Internet" to mean the myriad of computer and telecommunications facilities that make up the world-wide networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP), or any predecessor or successor protocols used to communicate information of all kinds by wire, radio, or other methods of transmission. *See* 16 C.F.R. § 312.2 (definition of "Internet"). The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.

Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule* [hereinafter *COPPA FAQ*], Question 6 ("What types of online transmissions does COPPA apply to?"), *www.ftc.gov/privacy/coppafaqs.shtm*.

[25] Operators of PI-collecting sites must:

Continued

A. The Difficulties in Obtaining "Verifiable Parental Consent"

In drafting the regulations that implemented COPPA (the "COPPA Rule"),[26] the Federal Trade Commission (FTC) in 1999 adopted a "sliding scale" approach to obtaining parental consent.[27] This approach allows operators of PI-collecting sites to use a mix of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, credit card authorizations and using encryption certificates.[28] The FTC has also authorized four "safe harbor" programs operated by private companies that help website operators comply with COPPA.[29]

In a February 2007 report to Congress about the status of the law and its enforcement, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online."[30] In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof."[31] The FTC attempts to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[32] This makes it clear that the FTC does not regard the methods the agency has prescribed for obtaining parental consent under COPPA as equivalent to strict age verification.

Although credit cards may seem the most robust tool for verifying parental consent (essentially, age verifying the parent), Federal courts have found, in rejecting the constitutionality of COPA, that, "payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards" and, although "payment card issuers usually will not issue credit and debit cards directly to minors without their parent's consent because of the financial risks associated with minors . . . there are many other ways in which a minor may obtain and use payment cards."[33]

B. "Collection": When Parental Consent is Required

COPPA requires that operators obtain verifiable parental consent "before any collection, use, and/or disclosure of personal information from children"—as well as for "any material change in the collection, use, and/or disclosure practices to which the parent has previously consented,"[34] subject to certain narrow exceptions.[35] Understanding how the COPPA Rule currently works and the pitfalls of COPPA expansion

---

Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information; . . . (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; (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; and (e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

16 C.F.R. § 312.3 (internal cross-references omitted).

[26] 16 C.F.R. Part 312. We use "COPPA Rule" when referring specifically to the FTC's implementing regulations, but use "COPPA" both to refer to the statute itself and to the scheme generally where appropriate.

[27] *See* Federal Trade Commission, *How to Comply with The Children's Online Privacy Protection Rule,* Nov. 1999, *www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm*.

[28] 16 C.F.R. § 312.5(b)(2). *See generally* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999), available at *www.ftc.gov/os/1999/10/64fr59888.pdf* [hereinafter 1999 *COPPA Order*]; *see also COPPA FAQ* supra note 24, Question 32 ("How do I get parental consent?").

[29] The four safe harbor programs are administered by the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo. *See* Federal Trade Commission, *Safe Harbor Program, www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html*.

[30] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 1, Feb. 2007, *www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf* [hereinafter *2007 COPPA Implementation Report*].

[31] *Id.* at 13.

[32] *Id.* at 12.

[33] *Gonzales,* 478 F. Supp. 2d at 801. COPA would have prohibited the online dissemination of material deemed harmful to minors under 17 for commercial purposes, 47 U.S.C. § 231(a)(1), subject to a safe harbor for sites that made a "good faith" effort to restrict access by minors: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology," 47 U.S.C. § 231(c)(1).

[34] 16 C.F.R. § 312.5(a).

[35] 16 C.F.R. § 312.5(c).

requires examining the three-pronged definition of "collection" created by the FTC, which COPPA itself left undefined.[36]

1. Requests from Sites

Most obviously, the COPPA Rule considers "collection" to occur each time a PI-collecting site requests "that children submit personal information online."[37] This requirement generally minimizes the amount of data collected from children and ensures that parents control the collection of information from their children.

2. Enabling Sharing of Personal Information

Less intuitively, the COPPA Rule considers "collection" to occur when a PI-collecting site merely "enabl[es] children to make personal information publicly available . . . *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."[38]

Unlike the first prong of "collection," consent is not required each time a communications tool is used to "make personal information publicly available," but merely for the child to gain access to the tool (*e.g.,* upon creation of a user account). Thus, the FTC intends to make parents gatekeepers over which sites their children join or participate in, rather than to give parents a veto right over every instance in which a child wants to share personal information (*e.g.,* by posting it to their profile or "wall" on a social networking site). Given the degree of interactivity on social networking sites, it is difficult to imagine how so granular a veto requirement could be feasibly implemented if COPPA were expanded.

What it means to make information "publicly available" is unclear. COPPA clearly requires consent before granting a child access to a site that would allow the child to "broadcast" personal information, such as by posting their name, photo, contact information, etc. such that the "public" can access that information, whether that means posting information to a social networking profile, on a website, or in a "public" chat room or message board (the latter two being the specific examples cited in COPPA and the COPPA Rule).[39] But does COPPA apply to communications that are not intended to be public? Would COPPA apply to a site that only allowed users to send "private" messages to each other? In short, how public is "public" enough that giving a child access to the underlying functionality would constitute collection? The FTC has never clearly answered these questions, but it has implied that it takes the "maximalist" view of what counts as collection: Allowing children to share personal information with *anyone,* even in one-to-one communications, constitutes "collection" subject to COPPA's parental consent requirement.[40] By contrast, the "minimalist" view would define "collection" in terms of the capability to "publish" or "broadcast" personal information such that it becomes "available" to anyone with access to the PI-collecting site. Which view a court would accept, if presented with

---

[36] The FTC has provided three definitions of "collection":

the gathering of any personal information from a child by any means, including but not limited to: (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.

16 C.F.R. § 312.2. *See also infra* at Section II.B.

[37] 16 C.F.R. § 312.2 (definition of "collection").

[38] *Id.*

[39] 15 U.S.C. § 6501(4)(B)(iv–v) (definition of "disclosure"); 16 C.F.R. § 312.2 (definition of "collection").

[40] In December 2007, the FTC added a question it its FAQ reflecting the agency's view that COPPA would require parental consent before allowing a child to send electronic greeting cards or forward items of interest to their friends. *COPPA FAQ supra* note 24, Question 44 ("My child-directed website wants to offer electronic post cards and the ability for children to forward items of interest on my site to their friends. Can I take advantage of one of the e-mail exceptions to parental consent?"). The FTC requires parental consent if users can "freely type messages in either the subject line of the e-card or in any text fields"—presumably, because this might lead to the sharing of personal information with the card's recipient. *See* Jim Dunstan, *E-cards and "Forward-to-a-Friend" Promotions: Not Kid Friendly Anymore, www.gsblaw.com/practice/notableevents.asp?StoryID=1137185152008&groupID=21; see also* Jim Dunstan, *FTC Issues Final Rules in CAN–SPAM Proceeding: Forward-To-A-Friend Promotion Mystery Solved, www.gsblaw.com/practice/notableevents.asp?StoryID=17866132008&groupID=21.*

a challenge to COPPA, is beyond the scope of this paper, but the ambiguity is worth noting.[41]

However broad the definition of "publicly available," the FTC's definition of "collection" to include the enabling of communication by children that might result in the any of personal information was itself controversial when the FTC first wrote the COPPA rules. The FTC (again) took a maximalist view of "collection,"[42] overriding the objections of free speech advocates who argued that Congress intended "to place duties on those who collect information from children" (in the normal sense of "collection" contained in the first prong of the definition) rather than "to regulate children's behavior" or "limit children's ability to speak."[43] These advocates proposed a minimalist definition of "collection" as "gathering, *by an operator,* of personal information," such that merely providing functionality like chat rooms and message boards would not constitute collection unless the operator actually gleaned personal information from such fora.[44]

3. Online Tracking & Cookies

Finally, COPPA would consider collection to occur through the use of persistent identifiers such as cookies[45] if 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."[46]

C. COPPA's Place in an Evolving Landscape

In the decade since Congress enacted COPPA, the kinds of information-sharing functionality governed by the "publicly available" prong of collection have exploded in popularity. New interactive communications tools and methods, now generally referred to as "social networking" capabilities, are a key hallmark of the "Web 2.0" era.[47] Of course, they had their precursors even in 1998, but the examples of such tools included in COPPA and the initial COPPA rule reveal just how much the web has evolved: "Chat rooms" and "message boards" certainly still exist but they have largely morphed into today's social networking sites (*e.g.,* Facebook, Myspace), which would have been unrecognizable in 1998, while services like blogging and micro-blogging (*e.g.,* Twitter) would have been inconceivable. Today, more users feel comfortable making personal information more "publicly available" than ever before, broadcasting their every thought and action, and even their exact physical location,[48] for all the world to see.

The growing ubiquity of "Web 2.0" tools has two implications. First, the sites currently covered by COPPA are growing ever more limited in their functionality relative to the rest of the Internet, as discussed be low.[49] For example, child-oriented sites must obtain verifiable parental consent before allowing children to send e-cards or use "Forward-to-a-Friend" functionality if the sites "permit the sender to enter her full name, her e-mail address, or the recipient's full name" or "provide users with the ability to freely type messages in either the subject line of the e-card or in any text fields."[50] Second, even under the minimalist view of "publicly available," expanding COPPA's age scope would affect far more websites today than it would have 11 years ago, because the functionality that constitutes "collection" (under the second prong of that term's definition) is now pervasive.

---

[41] The maximalist approach essentially reads the term "publicly available" out of the statute by construing collection to mean "available to anyone." Such a construction might, for example, violate the cannon of statutory interpretation against surplusage: "[T]he presence of statutory language 'cannot be regarded as mere surplusage; it means something.'" *Chickasaw Nation* v. *United States,* 534 U.S. 84, 97 (2001) (quoting *Potter* v. *United States,* 155 U.S. 438, 446 (1894)).

[42] *1999 COPPA Order, supra* note 28, at 59,889–890.

[43] Supplemental Comments of The Center for Democracy and Technology, The American Civil Liberties Union, and The American Library Association, filed in *Rulemaking to Implement the Children's Online Privacy Protection Act of 1998,* Aug. 25, 1999, at § I.B *www.ftc.gov/privacy/comments/supplementalcdtacluala.htm*.

[44] *Id.* (emphasis original, indicating proposed addition to the FTC's rule as originally proposed).

[45] 16 C.F.R. § 312.2 (definition of "collects or collection").

[46] 16 C.F.R. § 312.2 (definition of "personal information").

[47] Tim O'Reilly, *What Is Web 2.0?: Design Patterns and Business Models for the Next Generation of Software,* Sept. 30, 2005, *www.oreillynet.com/lpt/a/6228*.

[48] *See, e.g.,* Google Latitude, *www.google.com/latitude/intro.html;* loopt, *www.loopt.com;* Pelago, *http://pelago.com*.

[49] *See infra* at Section III.A.

[50] Absent such sharing, the FTC allows child-oriented sites to use COPPA's exception for one-time communications, found at 16 C.F.R. § 312.5(c). *See supra* note 40.

III. Does COPPA Really Work?

Before addressing the many challenges associated with COPPA 2.0 proposals, one must ask the critical—but ignored—threshold question: Is "COPPA 1.0" really working? To answer this question, one must first decide what COPPA 1.0 is supposed to accomplish. The original goals of COPPA, as expressed by its Congressional sponsors, were to:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[51]

Thus, as its name implies, COPPA is first and foremost about protecting the privacy of children. COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools . . . for becoming involved in and overseeing their children's interactions online."[52] However admirable, "protect[ing] the safety of children" is merely an indirect goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's direct goal). The FTC has attempted to blur this distinction, elevating child protection to a direct goal of COPPA.[53] Indeed, this was the primary reason the FTC adopted the maximalist definition of "collection" to include enabling communication (rather than direct gathering of personal information by operators), over-ruling free speech concerns.[54]

The FTC claims COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[55] Indeed, many of those advocating expansion of COPPA do so on the grounds that COPPA makes children safer online from sexual predators. What these advocates fail to acknowledge is that, to the extent COPPA has enhanced child safety—indeed, to the extent that COPPA can be effectively administered at all—it is because of the unique circumstances of the under-13 age bracket and the PI-collecting sites that have evolved to serve that community. In particular:

> 1. The functionality of child-oriented sites is usually tightly limited: They are closed, walled gardens;
>
> 2. Many smaller websites catering to children charge a fee for admission—even as fee-based models have withered away on the rest of the Internet; and
>
> 3. There are relatively few sites that cater exclusively to the under–13 crowd, which may be an unintended consequence of COPPA itself.

Each of these factors is discussed below, as relates to COPPA's perceived goals.

A. Child-Oriented Sites Limit Functionality

Child-oriented sites typically have very limited functionality: In essence, their operators intentionally "cripple" the sort of functionality found in most PI-collecting sites (especially social networking sites) geared toward older users. *That fact alone makes COPPA-covered sites far less likely to be subject to fraudulent entry or dangerous interactions:* Why would an adolescent or an adult predator ever want to gain access to a site that offers little more than drop-down menus and a few buttons to click on when interacting with others?

---

[51] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[52] *2007 COPPA Implementation Report, supra* note 30, at 28.

[53] The FTC has carefully—or perhaps simply carelessly—edited Congress's original statement of purpose: Where Congress had originally declared that COPPA was intended "*to enhance parental involvement* to help protect the safety of children [online]," 144 Cong. Rec. S11657 (emphasis added), the FTC has declared that COPPA was intended "to protect the safety of children [online]." *2007 COPPA Implementation Report, supra* note 30, at 3.

[54] The FTC based its adoption of the maximalist view of "collection" by noting that:

> children's use of chat rooms and bulletin boards that are accessible to all online users present the most serious safety risks, because it enables them to communicate freely with strangers. Indeed, an investigation conducted by the FBI and the Justice Department revealed that these services are quickly becoming the most common resources used by predators for identifying and contacting children.

1999 COPPA Order, supra note 28, at 59,890 (internal citations omitted). See also supra at 11 and note 43.

[55] *2007 COPPA Implementation Report, supra* note 30, at 28.

The primary reason that children are likely safer in those environments probably has less to do with COPPA's parental consent requirements and much more to do with the fact that most of the PI-collecting sites covered by COPPA are tightly controlled and highly moderated walled gardens with very limited functionality—a sort of "Junior Internet."

B. Child-Oriented Sites Charge Fees

While most Internet content and services are now "free" (*i.e.,* advertising-supported),[56] many child-oriented PI-collecting sites charge admission fees. There are several reasons they do so:

- "[R]equiring a parent to use a credit card in connection with a transaction" is among the methods for obtaining verifiable parental consent in the FTC's sliding scale.[57] The FTC requires that an operator charge some fee so that the credit card will be verified by its issuer and "because, through receipt of a monthly statement, the parent is given additional notice that the transaction occurred and has an opportunity to investigate any suspicious activity and revoke consent."[58]
- Commercial child-oriented sites must somehow recoup the costs of obtaining verifiable parental consent—estimated in 2005 at more than $45 per child.[59] Because COPPA limits operators' ability to effectively target advertising to children, thereby reducing the value of advertising inventory on PI-collecting sites, they usually must rely on direct fees.
- Many child-oriented sites rely heavily on constant human moderation and oversight, which necessitates a method of funding those workers.
- It is easier for child-oriented sites to continue charging small fees once they have a credit card on file (something most sites never accomplish) and because there is relatively less competition in the child-oriented marketplace than in the Internet generally.

Importantly, the more a site charges for access, the more likely it is that the parent or guardian pays attention to what their child is doing on that site. The hassle for parents of having to pay a fee gets parents thinking, and talking to their kids, about those sites, argues Denise Tayloe of Privo, one of the four FTC-approved providers of COPPA safe harbor age verification services.[60]

However, Tayloe has noted that one of the problems associated with the current COPPA regime is that "Children quickly learned to lie about their age in order to gain access to the interactive features on their favorite sites. As a result," she notes, "data bases have become tainted with inaccurate information and chaos seems to be king where COPPA is concerned."[61] The FTC, well aware that blocking access to children under 13 could simply encourage them to lie about their age, requires operators to "design [their] age collection input screens in a manner that does not encourage children to provide a false age in order to gain access to [their] site."[62] In particular, the FTC recommends "using a temporary or a permanent cookie to prevent children from back-buttoning to enter a different age."[63] But if children can learn to lie about their age, they can probably learn to delete cookies, too—since cookie deletion is a privacy feature now common in every browser.[64]

Despite these problems, Tayloe falls back on the original justification of COPPA: increasing parental involvement. Even though "there is no perfect solution" and it

---

[56] *See, e.g.,* Chris Anderson, *Free! Why $0.00 Is the Future of Business,* Wired, Feb. 25, 2008, *www.wired.com/techbiz/it/magazine/16–03/ff_free*. The most notable exception to this rule is Massively Multiplayer Online games such as World of Warcraft, which are also potentially subject to COPPA.

[57] 16 C.F.R. § 312.5(b)(2).

[58] *See COPPA FAQ, supra* note 24, Question 33 ("I would like to get consent by collecting a credit card number from the parent, but I don't want to engage in a transaction. Is this ok?").

[59] *See* Comments of Parry Aftab, Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children at 2, June 27, 2005, *www.ftc.gov/os/comments/COPPArulereview/516296–00021.pdf* [hereinafter *Aftab Comments*].

[60] Denise Tayloe, *It's Time to Comply with COPPA,* The Privacy Advisor, Vol. 6, No. 10, Oct. 2006, at 5.

[61] *Id.*

[62] *See COPPA FAQ, supra* note 58, Question 39 ("Can I block children under 13 from my general audience website?").

[63] *Id.*

[64] Adam Thierer, Berin Szoka & Adam Marcus, The Progress & Freedom Foundation, *Privacy Solutions,* PFF Blog, Ongoing Series, *http://blog.pff.org/archives/ongoing_series/privacy_solutions*.

is not possible to completely "stop a child from lying and putting themselves at risk," Tayloe believes that COPPA "provides a platform to educate parents and kids about privacy."[65] Providing a platform to educate parents and kids about online privacy or safety is certainly important, but there are other ways to do this besides imposing strict age verification mandates. Educational initiatives and public service announcements, for example, could also encourage greater parent-child interaction. Indeed, the courts have concluded that the First Amendment *requires* the government to utilize such educational initiatives as "less restrictive" alternatives to age verification technologies in other contexts.[66]

While we don't really have any idea what level of parent-child interaction COPPA incentivizes, or how many children (or adults) are able to gain access to PI-collecting sites under false pretenses, the key operational assumption on which COPPA rests is that by creating an added economic hurdle or barrier to entry (in the form of entry fees or the hassle of filling out paperwork or forms), COPPA gets some—maybe even most—parents to put more thought into what their kids are doing online, and that in turn somehow improves online child safety.

However useful COPPA might be in enhancing parental involvement, it does not necessarily mean that children are operating in perfectly "secure" or "verified" environments. COPPA wasn't primarily put on the books to prevent "bad guys" from interacting with children online; it was about minimizing the collection of children's personal information and giving parents control over collection of information from their children.[67] Thus, COPPA does not require excluding older users from child-oriented sites, some websites indeed may try to do so, building on COPPA's required age verification system, because of market demand from parents to exclude sexual predators. Of course, age verification is hardly fool-proof for either kids or adults. So, to the extent some "bad guys" are getting on those sites under false pretenses, both children and parents may be lulled into to a false sense of security after they are told the site is COPPA-verified—whether or not the site actually attempts to exclude older users and regardless of how effective the site may be in doing so. This may actually increase the danger of predation to children.[68]

C. Does COPPA Encourage Consolidation or Limit Competition?

As noted above, there are significant costs associated with the verifiable parental consent methods that PI-collecting sites must implement to comply with COPPA. If we are to fully understand the experience of COPPA as a regulatory model, we must consider the extent to which COPPA may have had the unintended consequence of limiting choice and competition by driving increased consolidation in the marketplace for child-oriented sites and services online—a question the FTC should consider answering. As early as 2001, even some Congressmen recognized this "unintended consequence" of COPPA in Congressional hearings on privacy.[69]

---

[65] E-mail from Denise Tayloe to Adam Thierer (Mar. 15, 2007) (copy on file with author).

[66] *See infra* at VI.A.3.

[67] *See supra* at 16.

[68] Internet security expert John Cardillo argues that even COPPA-compliant sites are vulnerable:

During an analysis of the security processes of certain sites we tested Imbee's. Our security team was able to create several fake children. More troubling was the inconsistency of the information used to do so. We used a fake name for the parent, a different fake name created for the Yahoo! e-mail account used at registration, and my credit card info (because the name on the CC is irrelevant). Fictional child, and three fake identifiers on supposedly the same adult. Not one red flag was raised, and we were allowed onto the site without a problem. Our team was able to do this multiple times. Had we been a real bad guy, we could have, at any time, chatted with other kids on the site as a child. One of several different children actually. Not only isn't it a security solution, it's downright dangerous.

E-mail from John J. Cardillo to Adam Thierer (March 11, 2007) (copy on file with author). Cardillo's findings thus make it clear how real predators intent on doing harm to children could exploit age verification processes designed to exclude adults from a supposedly "teens-only" site (just as predators already do with sites supposedly limited to kids under 13). Indeed, because many predators have children of their own, they might use this approach to obtain an ID for their own kids and then go online under their child's name to prey on other children. The fiction that all users of a site are "verified" creates a false sense of security—a serious problem for child safety. As Cardillo has noted elsewhere, predators who create a "pedophile passport" could operate freely in supposedly "safe and secure" environments. See Adam Thierer, The Progress & Freedom Foundation, *Age Verification for Social Networking Sites: Is It Possible? Is It Desirable?,* Progress on Point 14.8, May 2007, at 6, *www.pff.org/issues-pubs/pops/pop14.8agverificationtranscript.pdf.*

[69] Rep. Billy Tauzin (R–LA) noted that COPPA "has now forced companies to discontinue a number of products targeted toward children" and asked "If we end up forcing private companies and nonprofits to eliminate beneficial products such as crime prevention material, have we

Continued

Of course, it could be the case that there are other reasons that there are relatively few sites catering exclusively to children. Nonetheless, as discussed below, it's worth considering how expanding COPPA might lead to more consolidation in the marketplace or how it discourages greater entry by smaller "mom-and-pop" sites that could cater to children. As noted by Parry Aftab, Executive Director of the children's advocacy group Wired Safety, "COPPA wasn't responsible for the demise of these sites, but when combined with the other factors [it] tipped the balance."[70] She concludes, appropriately:

> It is crucial that at this tentative stage for the kids Internet industry we don't do anything to make its survival more difficult. We should be looking at easy to encourage safer communities for preteens and innovations to help create fun, entertaining and educational content for kids online.[71]

IV. What if COPPA Were Expanded to Cover Adolescents?

However effective COPPA might be in fulfilling its purposes, and whatever its unintended consequences, the COPPA Rule's requirements are *relatively* easy for the private sector to implement and for the government to enforce because, as mentioned, they apply only to the collection of information about children under 13 by commercial operators only when (i) the operator's PI-collecting Site or service is "directed to children" or (ii) the operator has actual knowledge that they are collecting personal information from a child. But how well would the COPPA approach "scale up" to the 13–17 age bracket?

The key practical difficulty in implementing a COPPA 2.0 system for adolescents is in the anonymity inherent in the technical architecture of the Internet. To quote a memorable cartoon from *The New Yorker* of all time: "On the Internet, nobody knows you're a dog."[72] Because website operators generally do not know who is accessing their site, requiring any special treatment of minors (*e.g.,* parental consent prior to the collection of personal information, access to the child's user profile) is tantamount to requiring age-verification of all users.[73]

Because "child-oriented" websites are generally easy to define and are very rarely used by adults, COPPA 1.0s age verification mandate has not significantly impacted the free speech rights of adults. But it is *far* more difficult to define a class of "adolescent-oriented" websites (as proposed in New Jersey) that are not also used by significant numbers of adults. Indeed, the Illinois bill does not even attempt to do so, defining its scope not in COPPA's "directed at" terms but purely in terms of site functionality.[74] In this sense, the Illinois bill is more restrictive than the New Jersey bill, since it would apply to sites with a certain functionality regardless of to whom they are "directed at." On the other hand, the New Jersey proposal is far more sweeping, since it applies to any site that collects user information if the site is "directed at" adolescents.[75] Whichever bill might ultimately affect more websites, the practical result of both COPPA 2.0 proposals is the same: They would, without

---

done a good thing? If teen-friendly sites, those that totally respect the privacy of the users stop offering e-mail services to children, is that a good thing? An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing of the House Committee On Energy and Commerce, 107th Cong. 6 (April 3, 2001) (statement of Rep. Tauzin.), available at *http://republicans.energycommerce.house.gov/107/action/107-22.pdf.*

[70] *Aftab Comments, supra* note 59, at 3.

[71] *Id.*

[72] Peter Steiner, *On the Internet, Nobody Knows You're a Dog, The New Yorker,* July 5, 1993 at 61, available at *www.unc.edu/depts/jomc/academics/dri/idog.html* (cartoon of a dog, sitting at a computer terminal, talking to another dog).

[73] Of course, the COPPA's second prong of age-verification requirement applies only when the website operator has "actual knowledge" that the user is a minor. *See supra* at 7 & note 22.

[74] The Illinois Bill defines a "social networking site" as:

an Internet website containing profile web pages of the members of the website that include the names or nicknames of such members, photographs placed on the profile web pages by such member, or any other personal or personally identifying information about such members and links to other profile web pages on social networking websites of friends or associates of such members that can be accessed by other members or visitors to the website. A social networking website provides members of or visitors to such website the ability to leave messages or comments on the profile web page that are visible to all or some visitors to the profile web page and may also include a form of electronic mail for members of the social networking website.

SNWARA, supra note 11, §5. This definition seems almost tailor-made for MySpace and Facebook: The second sentence of the definition would exclude sites like LinkedIn, which includes profiles but does not allow users to post public comments on other users' profiles. While this focus on specific site functionality seems to differ from COPPA's approach, in fact it does little more than apply COPPA's second definition of "collection" as "Enabling children to make personal information publicly available." See 16 C.F.R. § 312.2 (definition of "collection"); *see also supra* at 8.

[75] *See supra* note 13.

explicitly saying so, require age verification of a large numbers of adults. This raises profound First Amendment concerns—particularly about the right of Americans to speak and receive information anonymously online.[76]

V. The Differences Between Children (0–12) & Adolescents (13–17)

Before examining these First Amendment concerns (which are more directly apparent in the case of the Illinois proposal), one must ask how they arise in the case of the more complicated New Jersey proposal, which applies to PI-collecting sites "directed at" adolescents.[77] This examination reveals the fundamental flaw in *any* attempt to extend COPPA to cover adolescents: COPPA 1.0 works only because of the unique characteristics of the under–13 age bracket.

A. Subjective Assessments about Intended Audiences Are Significantly Easier for Children than for Adolescents

In determining whether a PI-collecting Site or service is "directed at children," the FTC considers the site or service's "subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children . . . and whether a site uses animated characters."[78] The following excerpts from FTC complaints illustrate how the agency has applied these criteria:

> The . . . subject matter [of *www.lilromeo.com*] is Lil' Romeo, a twelve-year-old recording artist who "enjoys 'just being a regular kid.'" The website features content directed to children such as an animated game in which the player helps Lil' Romeo save an elementary school from aliens by answering simple math and history questions. The website also features music and lyrics from Lil' Romeo's album "Game Time," which is "about having fun, and also about, you know, kids['] things . . ."[79]

And:

> Defendant operates the *www.etch-a-sketch.com* website, which provides information about its toys, including the "Etch A Sketch" drawing toy. The subject matter, visual content, and language of this website are directed to children under the age of 13. For example, the site features a cartoon character named "Etchy"—an Etch A Sketch sporting sunglasses, purple hair and legs. Etchy invites visitors to play "cool games," such as drawing with an online Etch A Sketch, finding hidden numbers, letters and shapes, and coloring pictures of Etchy and friends. The site also contains an "interactive story" titled, "Etchy Goes to a Birthday Party."[80]

The FTC settled both cases with consent decrees—like, apparently, all the FTC's COPPA enforcement actions.[81] These examples demonstrate that subjective standards can sometimes work reasonably well in certain contexts. As Justice Potter Stewart famously said of obscenity, "I know it when I see it."[82] The same could probably be said, in many cases, about what constitutes child-oriented content; and this approach seems to have worked well enough for the FTC's COPPA enforcement efforts. But how well, if at all, would such a standard work in determining the scope of COPPA 2.0 proposals (like New Jersey's) that retain COPPA's requirement that a site be "directed at" a certain audience when that audience is not children (0–12) but adolescents (13–17)?[83]

Any regulatory system that, like COPPA, rests on age stratification inevitably requires the drawing of arbitrary boundaries. But ultimately, *some* age must be chosen. Whatever the differences between 12 and 13, the differences between 12

---

[76] Adam Thierer, The Progress & Freedom Foundation, *USA Today, Age Verification, and the Death of Online Anonymity,* PFF Blog, Jan. 23, 2008, *http://blog.pff.org/archives/2008/01/usa_today_doesn.html*.

[77] Like COPPA, New Jersey's AOPPA bill also applies to cases of actual knowledge that an operator is collecting personal information from an adolescent. *See supra* note 13.

[78] 16 C.F.R. § 312.2 (definition of "website or online service directed to children").

[79] *U.S.* v. *UMG Recordings, Inc.,* Civil Action No. CV–04–1050, Complaint at 4–5 (C.D. Ca. 2004), *www.ftc.gov/os/caselist/umgrecordings/040217compumgrecording.pdf*.

[80] *U.S.* v. *The Ohio Art Company,* Complaint, ¶ 12 (N.D. Oh. 2002), *www.ftc.gov/os/2002/04/ohioartcomplaint.htm*.

[81] *See* Federal Trade Commission, *Children's Privacy Enforcement Cases, www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html* (including a consent decree for each case).

[82] *Jacobellis* v. *Ohio,* 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[83] While New Jersey's proposal retains this approach, hewing closely to COPPA's current structure, *see supra* note 13 and accompanying text , Illinois's proposal drops the concept and simply applies to all sites with certain social networking functionality, *see supra* note 11.

(COPPA's ceiling) and 17 (the ceiling established in some COPPA 2.0 measures) are significant. Although the original version of the COPPA legislation would have required "reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information" for kids 13–16, the legislation never required verifiable parental consent for minors above 12.[84] The FTC explains Congress's rationale for this distinction as follows:

> Congress and industry self-regulatory bodies have traditionally distinguished children aged 12 and under, who are particularly vulnerable to overreaching by marketers, from children over the age of 12, for whom strong, but more flexible protections may be appropriate. In addition, distinguishing adolescents from younger children may be warranted where younger children may not understand the safety and privacy issues created by the online collection of personal information.[85]

Thus, it appears that Congress was simply following a long-standing distinction based on the cognitive capabilities of children under 13. But whether anyone realized it at the time, this distinction has proved essential for the administration of COPPA as a statute that defines its scope by the audience to which sites are "directed." Whenever the "tipping point" in cognitive capabilities occurs, the age of 13 roughly corresponds to an important point of departure in psychological growth between "childhood" and "adolescence."

This moment was best described two thousand years ago by the Apostle Paul of Tarsus, when he wrote, "When I was a child, I spake as a child, I understood as a child, I thought as a child: but when I became a man, *I put away childish things.*"[86] Paul equated what we think of as "adolescence"—a profoundly modern invention[87]—with adulthood. Paul had no more conception of "adolescence" than did Shakespeare, who—like Congress with COPPA—chose thirteen as the age of Juliet, his greatest star-crossed lover.[88] But Paul offered perhaps the best reason why COPPA's scope ends at thirteen: this is the roughly point at which minors begin to shun "childish things"—say, losing interest in Club Penguin in favor of more "grown-up" sites like MySpace or Facebook. If one has to choose a clear bright line rule as to when, on average, that shift occurs, 13 seems to be about as accurate as any. (Indeed, modern Jews—like the Jewish Paul before them—continue to recognize this as the threshold of maturity by generally holding a Bar Mitzvah for boys at age 13, and a Bat Mitzvah ceremony for girls at age 12.[89]) This is less a question of how much protection minors of any particular age require, and more a question of when their interests change: At about this age, adolescents begin to share interests with adults in ways that children 12 and below do not; if left to their own de-

---

[84] *See supra* note 14 and associated text.

[85] *COPPA FAQ, supra* note 58, Question 8 ("Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?"), *www.ftc.gov/privacy/coppafaqs.shtm*. The FTC also reminds companies:

> websites' information practices regarding teens and adults are subject to Section 5 of the FTC Act, which prohibits unfair or deceptive acts and practices. See Staff Opinion Letter to Center for Media Education (July 15, 1997) for guidance on how Section 5 applies to information practices involving teens. In addition, recent concern about the risks of child participation on social networking websites led the FTC to issue a set of safety tips for social networking. See "Social Networking Sites: A Parents' Guide" (September 2007), available at *www.ftc.gov/opa/2006/05/socialnetworking.shtm; see also www.onguardonline.gov/docs/onguardonline_socialnetworking.pdf*.

[86] *The First Epistle of Paul the Apostle to the Corinthians* 13:11 (King James), available at *www.bartleby.com/108/46/13.html* (emphasis added).

[87] Sociologist Rowan Wolf explains:

> [F]or much of the history of human society, there has not really been the concept of "childhood" as we know it today. Once a child was able to speak and eat on its own, it was essentially considered a miniature adult capable of participating in a limited way in the survival of the family. Once "children" hit puberty, they were considered adults, though they might not take on adult roles until they formed their own family. There was no concept of adolescence. . . . Children went from "miniature adults" expected to act like adults but without the rights of adults, to a carefree, dependent period of exploration and learning. When we look at the expectations of "teenagers," we define this as a rebellious period of individuation. We simultaneously expect adolescents to act like adults and rebel from them at the same time. This is a period where people are sexually mature, but socially and economically dependent.

Age Stratification, Sept. 2005, *www.srwolf.com/wolfsoc/articlearchives/2008/11/age_stratification.html*.

[88] *See, e.g., The Invention of Adolescence,* Psychology Today, Jan./Feb. 1995, *www.psychologytoday.com/articles/pto–19950101–000024.html*.

[89] *See, e.g., Bar Mitzvah, Bat Mitzvah and Confirmation,* Judaism 101, *http://www.jewfaq.org/barmitz.htm*.

vices, adolescents would spend far more time on "general audience"[90] websites than would children. Thirteen is probably about the point at which this transformation begins to accelerate. But regardless of precisely when it happens, it should be apparent that the sites favored by adolescents 13 and over will be difficult to distinguish as "adolescent-oriented" because they are rarely, if ever, as thoroughly dominated by adolescents as "child-oriented" sites are by children 12 and under. This problem gives rise to the significant constitutional concerns raised by COPPA 2.0 proposals.

B. The Difficulties of Empirical Assessments about Intended Audiences

If the subjective "I know it when I see it standard" is not so easily applied for determining what constitutes adolescent-oriented PI-collecting sites, the alternative under the FTC's COPPA rules is to examine "competent and reliable empirical evidence."[91] Could demographic data about a site's membership provide sufficiently clear guidance about the scope of a law that (like New Jersey's proposal) retains COPPA's current "directed at" approach?[92]

The FTC has never addressed the difficult question of setting a minimum threshold of child membership/participation in a site above which the site would be considered "directed at children:" Not one of the complaints brought by the FTC under COPPA cites demographic evidence. Because, as discussed above, child-oriented websites tend to exist in a virtually distinct "Junior Internet," with little overlap between adults and children, and because many parents use technological controls to keep their children (but not their adolescents) within this Junior Internet, it is hardly surprising that the FTC has never answered this question: Subjective criteria are generally sufficient to identify child-oriented sites, and those sites are likely to be used overwhelmingly by children or young adolescents with very little adult participation.

But as discussed above, few of the websites frequented by adolescents are dominated so overwhelmingly by adolescents as children dominate the membership of the Junior Internet to which COPPA currently applies. Instead, adolescents participate in many of the same PI-collecting sites used by adults, as demonstrated by the following sample of some of the more popular Web 2.0 sites, including demographic estimates:

Exhibit 1: Popular Web 2.0 Sites[93]

Site Name	Unique U.S. Users	Annual U.S. Page Views	% of Users Under Age 18
myyearbook.com	2,000,000	860,000,000	50.00%
bebo.com	2,400,000	340,000,000	35.00%
nickjr.com	2,400,000	210,000,000	31.67%
myspace.com	67,000,000	43,000,000,000	28.36%
photobucket.com	25,000,000	1,300,000,000	26.80%
movie6.net	1,100,000	24,000,000	26.36%
fanpop.com	1,100,000	16,000,000	21.82%
xanga.com	1,600,000	82,000,000	20.00%
tagged.com	3,500,000	1,100,000,000	19.71%
zango.com	2,900,000	21,000,000	17.93%
aol.com	37,000,000	4,000,000,000	16.49%
hi5.com	2,800,000	870,000,000	15.00%
facebook.com	74,000,000	30,000,000,000	12.16%
yahoo.com	140,000,000	36,000,000,000	11.43%
friendster.com	1,600,000	490,000,000	11.25%
wordpress.com	23,000,000	300,000,000	10.43%
gametrailers.com	1,200,000	50,000,000	10.00%
flickr.com	21,000,000	1,000,000,000	9.52%

So would some of these sites be considered "adolescent-oriented" even though most of their users are actually adults? Perhaps not in New Jersey (depending on

[90] The term "general audience" is commonly used instead of "adult-oriented" for content that is not directed at children.

[91] 16 C.F.R. § 312.2 (definition of "website or online service directed to children").

[92] *See supra* note 13.

[93] Data obtained from Google Ad Planner on Mar. 1, 2009, *https://www.google.com/adplanner/planning* (by dividing "UV users" for the 0–17 "audience" by "UV users" for the entire population).

the circumstances of any particular site),[94] but this is essentially what the Illinois bill requires:[95] The approximately 88 percent of Facebook's users 18 and above must be age verified for the sake of obtaining parental consent for the 12 percent under 18. This example is apt, because 12 percent happens to coincide with the estimated percentage of American Internet users under 18: 12.6 percent or 28 million Americans.[96]

C. Possible Reactions to COPPA 2.0s Uncertain Scope

Of the top 250 sites ranked by audience reach, only a handful stand out as being obviously child-oriented, such as *cartoonnetwork.com* and *nick.com* (Nickelodeon). A number of leading social networks top the list and many, if not most, of these sites require the sharing of some personal information (if only an e-mail address) for full functionality. But how would *any* of these operators—let alone the millions of sites in the "Long Tail" of Internet content—determine whether they would be considered adolescent-oriented? By the same token, how should a legislator following Illinois's approach (defining the scope of the COPPA 2.0 law in terms of site functionality) decide which features should trigger age verification requirements?

To the extent PI-collecting Site operators might be unsure whether a COPPA 2.0 age verification mandate would apply to them, they would likely take one of the following steps to minimize their potential liability.

1. Trying to Block All Adolescents

Of course, since PI-collecting Site operators do not know which would-be users are minors without an age verification system (and perhaps not even then!), the most they could do would be to *claim* that they block access by adolescents. Websites can certainly try to block users who initially admit to being under 18 from trying to register again for the site.[97] But this approach is only effective to the extent that adolescents are naïve enough to admit their true age in the first place and not to know how to circumvent whatever system the operator has in place for preventing users from trying to register for the site after initially being blocked—which should be relatively simple to do (*e.g.,* by deleting cookies from the site).

2. Avoiding Actual Knowledge

Some PI-collecting Site operators may give up on the "directed at" prong and try to avoid gaining "actual knowledge" that a user is under 18 simply by ceasing to ask for age information upon the creation of a user account—or perhaps by no longer requiring the creation of user accounts altogether. But this is a dangerous gamble because, if a site is ultimately found to be "adolescent-oriented," *not* asking for age upon sign-up might be considered a serious violation in itself.[98] This "Catch-22" places site operators in a difficult and legally precarious position—especially significant smaller site operators trying to raise funding.

Other operators may reduce human moderation of their site in order to avoid situations in which an employee might learn that a user is under 18 (*e.g.,* by reading their comments or profile). This is precisely the sort of perverse incentive that Congress attempted to avoid in passing Section 230 of the Communications Decency Act of 1996, which fully immunized online intermediaries from liability even if they made "good Samaritan" efforts to self-police their sites for objectionable content.[99] (The FTC has already created this perverse incentive under COPPA, but given the demand among parents for heavy moderation on child-oriented sites, COPPA's perverse incentive may have had little effect.[100]) Thus, COPPA 2.0 proposals could lead

---

[94] *See supra* note 13 and at 17.

[95] *See supra* note 74.

[96] Data obtained from Google Ad Planner on Mar. 1, 2009, *https://www.google.com/adplanner/planning* (by limiting age to 0–17).

[97] *See supra* at 29.

[98] For example, the amount of a penalty imposed on an operator deemed to be in violation would depend on "Respondent's good faith" and "The deterrent effect of the penalty action." 16 C.F.R. § 1.67(b) & (d).

[99] "No provider or user of an interactive computer service shall be held liable on account of . . . any action taken to enable or make available to information content providers or others the technical means to restrict access to material . . . material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable. . . ." 47 U.S.C. § 230(c)(2).

[100] *See COPPA FAQ, supra* note 58, Question 41(b) ("What happens if a child visits a chat room or creates a blog and announces his or her age?"). The FTC answers: "You may be considered to have actual knowledge with respect to that child if someone from your organization sees the post, or if someone alerts you to the post (for example, a concerned parent who learns that his child is participating on your site). However, if no one in your organization is aware of the post, then you may not have the requisite actual knowledge under the Rule." *Id.*

to less protection for minors, not more, by discouraging site operators from "chaperoning" interaction on their sites.[101]

3. Age-Verifying All Users

COPPA 2.0s greatest threat is that large numbers of PI-collecting Site operators would be—or would feel—compelled to require age-verification of large numbers of adults as users. There is currently no age verification requirement other than COPPA, which affects adults only to the extent that parents need to establish their parental relationship to their kids. But COPPA affects few other adults because few adults want to use child-oriented PI-collecting sites like Disney's Club Penguin. COPPA 2.0 proposals would either *directly* require age verification of all adults who wanted to use "social networking sites" (as proposed in Illinois) or *indirectly* require much the same thing by mandating age verification for "adolescent-oriented sites" (as proposed in New Jersey). Indeed, this may be precisely what some COPPA 2.0 advocates want, since they may envision it as the only way to make the Internet truly "safe" for adolescents.

But few proponents would make such a goal explicit, for they know that such a "scaled-up" COPPA would essentially converge with COPA as a broad age verification mandate. As noted below, this highlights the First Amendment implications of trying to turn COPPA into something it was not designed to be: not merely a tool for enhancing parental involvement and kids' privacy, but a broad mandate for child safety.

VI. The First Amendment Implications of Broad Age Verification Mandates

Both COPPA and COPA rest on a stratification of users by age, but the approach of the two laws is very different: While COPPA requires age verification if content is "directed at" minors under age 13, COPA would have required that *all* website operators restrict access to material deemed "harmful to minors" by minors under the age of 17 and therefore requires age verification of *all* users who attempt to access such content (in order to identify minors). COPPA is focused on certain kinds of potentially harmful *contacts*[102] while COPA is focused on potentially harmful *content*.[103]

But by expanding the age range of COPPA to include adolescents, COPPA 2.0 proposals essentially converge with COPA, reaching the same practical consequence: age verification mandates for large numbers of adults *as users* (not as parents). Only the scope of sites covered by the laws is different: under COPA, sites deemed "harmful to minors," and, under COPPA 2.0, adolescent-oriented or certain social networking sites. Thus, to the extent that COPPA 2.0 proposals require age verification of adults, they would be subject to constitutional attacks similar to those against COPA. But COPPA 2.0 proposals would also burden the rights of adults to communicate with adolescents and the free speech rights of adolescents.

Finally, the fact that COPPA (like COPA) applies only to commercial sites would do little to protect it from constitutional attack, because in a world of user-generated content, the commercial nature of a site has little to do with the commercial/non-commercial nature of the speech carried on it. For example, obviously commercial sites like MySpace and Facebook serve as platforms for a wide variety of not-for-profit and political communications.

A. First Amendment Rights of Adults

After a decade-long court battle over the constitutionality of COPA, the U.S. Supreme Court in January 2009 rejected the government's latest request to revive the law, meaning it is likely dead.[104] Three of the key reasons the courts struck down COPA would also apply to COPPA 2.0 proposals.

1. Anonymous Speech Rights of Adults

COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are

---

[101] *See infra* at 30.

[102] *See supra* at 9.

[103] COPA makes it illegal to "knowingly . . . make[ ] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. 231.

[104] *See* Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA,* PFF Blog, Jan. 21, 2009, *http://blog.pff.org/archives/2009/01/closing_the_boo.html. See also* Alex Harris, *Child Online Protection Act Still Unconstitutional, http://cyberlaw.stanford.edu/packet/200811/child-online-protection-act-stillunconstitutional.*

simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial."[105] In 2008, in striking down COPA for the third and final time, the Third Circuit approvingly quoted the district court, which had noted that part of the reason age verification requirements deterred users from accessing restricted content was "because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet."[106] The district court had held that:

> Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material privately and anonymously, especially if it is sexually explicit. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.[107]

The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Great works of literature have frequently been produced by authors writing under assumed names. Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[108]

By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves more protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz.,* pornography), COPPA 2.0 would burden access to material by adults as well as minors not because that material is harmful or obscene but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications about political nature, which deserved the highest degree of First Amendment protection.

2. Speech Rights of Site Operators

The necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is that COPPA 2.0, like COPA, would necessarily reduce the audience size of PI-collecting sites subject to age verification mandates. Furthermore, such mandates would encourage websites to self-censor themselves to avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate—or to legal liability if they fail to implement age verification. The substantial cost of age verification could significantly impact, if not make impossible, the business models of many PI-collecting sites, which generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[109]

---

[105] *American Civil Liberties Union* v. *Ashcroft,* 322 F.3d 240, 259 (3d Cir. 2003) (*ACLU II*).

[106] *American Civil Liberties Union* v. *Ashcroft,* 534 F.3d 181, 196 (3d Cir. 2008) (*ACLU III*) (*Gonzales,* 478 F. Supp. 2d 775 at 806).

[107] *Gonzales* at 805.

[108] *McIntyre* v. *Ohio Elections Comm'n,* 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also Talley* v. *California,* 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

[109] *See ACLU III,* 534 F.3d at 196–97 (citing *Gonzales* at 804). The Court held that websites "face significant costs to implement [COPA's age verification mandates] and will suffer the loss of legitimate visitors once they do so." *Id.* at 197.

3. Less Restrictive Alternatives to Regulation

The Third Circuit drew on the Supreme Court's 2004 decision striking down COPA on the grounds that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[110] Similarly, parental control software already empowers parents to restrict their kids' access to PI-collecting sites. (It's particularly easy for parents to restrict access to the leading social networking sites that seem to be driving so much of the push for COPPA 2.0, so that their kids.)

Thus, the free speech rights burdened COPPA 2.0 proposals are at least as important as those burdened by COPA, and blocking software already empowers parents to restrict their kids' access to PI-collecting sites, just as it allows parents to restrict access to pornography. Of course, if COPPA 2.0 laws were actually enacted and subject to legal challenge, the outcome of the case would depend largely on the level of constitutional scrutiny involved. COPPA 2.0 advocates might argue that, whatever the rights at stake, a lower level of constitutional scrutiny should apply because COPPA 2.0 does not target a special category of content. If true, this could mean that, although age verification mandates to restrict access to "harmful" material are unconstitutional, far more sweeping mandates restricting access to non-harmful information *could* be constitutional. Such inconsistency is indeed a perverse consequence of the fact that our First Amendment jurisprudence focuses not on the rights at stake, but on whether a regulation is "content-neutral" in deciding what level of scrutiny to apply—which, in turn, often determines the outcome of the case.[111] But in this case, COPPA 2.0 proposals likely *would* be subject to strict scrutiny to the extent that they are, like COPA, focused on a certain category of content: that "directed at" adolescents (rather than "harmful to minors").

Legislators who attempt to escape strict scrutiny by defining the scope of their bill (as in Illinois) not by its targeted audience but by reference to specific functional capabilities (in the definition of "social networking site")[112] will likely find that a court will see through such window-dressing: If they recognize that such bills are nonetheless aimed at a certain category of adolescent-oriented content, they will apply strict scrutiny anyway. But even under intermediate scrutiny, COPPA 2.0 proposals would be subject to serious attack.

B. First Amendment Rights of Adolescents

In addition, in COPPA 2.0 approaches, the government would restrict the ability of adolescents to access content, not because it could be harmful to them or because it is obscene, but merely because it is "directed to" them. While the First Amendment rights of minors may not be on par with those of adults, adolescents *do* have the right to access certain types of information and express themselves in certain ways.[113] The Supreme Court has held that "constitutional rights do not mature and come into being magically only when one attains the state-defined age of majority."[114] It remains unclear how an expanded COPPA model might interfere with the

---

[110] *Id.* at 198 (quoting *ACLU* v. *Mukasey,* 534 F.3d 181, 198 (2008)).

[111] Ashutosh Avinash Bhagwat, *The Test that Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence,* 2007 U. Ill. Law. Rev. 783 (2007), available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=887566.*

[112] *See supra* note 74.

[113] *See* Theresa Chmara & Daniel Mach, *Minors' Rights to Receive Information Under the First Amendment,* Memorandum from Jenner & Block to the Freedom To Read Foundation, Feb. 2, 2004, *www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/minorsrights.cfm* (summarizing case law regarding minors' first amendment rights, especially in schools and in the context of mandates that public libraries filter Internet content); *United States* v. *American Library Ass'n,* 123 S. Ct. 2297 (2003), available at *laws.findlaw.com/us/000/02-361.html* (upholding the constitutionality of a filtering software system applicable to minors); *see generally, Tinker* v. *Des Moines Ind. Comm. School Dist.,* 393 U.S. 503 (1969) (upholding students' rights to wear protest armbands and affirming that minors have speech rights) available at *www.oyez.org/cases/1960–1969/1968/1968_21;* cf. *Morse* v. *Frederick,* 551 U.S. 393 (2007), available at *www.oyez.org/cases/2000-2009/2006/2006_06_278/* (holding that the First Amendment rights of students in school and at school-supervised events are not as broad as those of adults in other settings).

[114] *Planned Parenthood of Cent. Mo.* v. *Danforth,* 428 U.S. 52, 74 (1976) (minors' right to abortion). *See also Bellotti* v. *Baird,* 443 U.S. 622, 635 n.13 (minors possess close to the "full capacity for individual choice which is the presupposition of First Amendment guarantees"); Catherine Ross, *An Emerging Right for Mature Minors to Receive Information,* 2 U. Pa. J. Const. L. 223 (1999); Lee Tien & Seth Schoen, Reply Comments of the Electronic Frontier Foundation filed in *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming,* MB Docket No. 0926, Federal Communications Commission,

Continued

First Amendment rights of adolescents, but it is clear that privacy and speech rights would come into conflict under COPPA 2.0, as they do in other contexts.[115]

For example, how might the parental-consent based model limit the ability of adolescents to obtain information about "safer sex" or how to deal with trauma, depression, family abuse, or addiction. Would an abusive father authorize a teen to visit a website about how to report child abuse? Would a parent of an adolescent struggling with their sexual identity let their kid participate in a self-help social networking page for gay and lesbian youth?[116] What rights are at play here and how do we reconcile them?

Maintaining the ability of kids to participate online interactions goes beyond content that most people would recognize as "serious"—from the perspective of both First Amendment values and the education of children. As a recent MacArthur Foundation study of the online youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[117]

It was at least in part in recognition of such difficult First Amendment questions that Congress removed the requirement in the initial legislative draft of COPPA that would have required PI-based sites to "use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[118]

Even if parents have an absolute right to block their adolescents' access to such data, they can already exercise that right by applying strict controls on the computers in their home. COPPA 2.0 proposals go well beyond recognizing this right by setting the default to "parental consent required" for adolescents to access a wide range of content—meaning that parents must "opt-in" on behalf of their children before their children can participate in PI-collecting sites. This, in turn, burdens the ability of adolescents to communicate, because their parents might censor (rightly or wrongly) certain information, or simply fail to understand the technologies involved or to be actively engaged. But whatever the free speech rights of adolescents, if anyone should be interfering with those rights, it should be their parents—not the government.

Some parents may object that, however effective parental control software may be in the home, it does not allow parents to control what their kids' access *outside* the home. This argument is understandable on some level, but in the end, it amounts to a demand that roadblocks be put up everywhere for the sake of particularly sensitive parents at the expense of everyone else in society, including potentially huge numbers of adult users—and of online anonymity in general.

May 18, 2009, *http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520216901*.

[115] *See generally* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach,* 11 Fordham Intell. Prop. Media & Ent. L.J. 97 (2000), available at *http://law.fordham.edu/publications/articles/200flspub6588.pdf;* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You,* 52 Stan. L. Rev. 1175 (2000), available at *www.law.ucla.edu/volokh/privacy.htm*.

[116] "There are parents who, for a variety of reasons (political, cultural, or religious beliefs, ignorance of the facts, fear of being exposed as abusers, etc.), would deliberately prevent their teens from accessing social-network sites (SNS)." *ISTTF Final Report, supra* note 8, Appendix F, Statement of Connect Safely, at 262 (listing examples of unintended consequences of age verification mandates).

[117] John D. and Catherine T. MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project,* at 2 [hereinafter MacArthur Study] *http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf*.

[118] This requirement was contained in the original bill, *supra* note 14 § 3(a)(2)(A)(iii), but was removed when that bill was reintroduced in its final form. In the interim, Congress held a hearing at which testimony was offered by, among others, Deirdre Mulligan of the Center for Democracy and Technology, which generally supported COPPA but argued for the very revisions that were ultimately made. In particular, Mulligan argued that:

Under the bill each time a 15 year old signs-up to receive information through e-mail his or her parent would be notified. For example if a 15 year old visits a site, whether a bookstore or a women's health clinic where material is made available for sale and requests information about purchasing a particular book or merely inquires about books on a particular subject (abuse, religion) using their e-mail address the teenager's parent would be notified. This may chill older minors in pursuit of information.

Mulligan Testimony, supra note 15.

But Illinois's COPPA 2.0 proposal goes even further, not merely expanding COPPA to cover a particular variety of social networking sites,[119] but requiring that such sites "allow the parent or guardian of the minor unrestricted access to the profile web page of the minor at all times."[120] Congress considered just such a parental access mandate in the initial draft of COPPA legislation back in 1998, but ultimately removed it from the final version of the legislation,[121] apparently because even some of COPPA's supporters worried, given the bill's initial application to the 13–16 age bracket, that "The establishment of a parental right to access all personal information about a teenager may intrude on older minors' privacy, rather than protect."[122]

C. Communication between Adolescents & Adults

Finally, COPPA 2.0 could infringe on the free speech rights of adults to communicate with adolescents online by driving PI-collecting sites to segregate users by age or to attempt to block access by adolescents. The vast majority of adult-minor interactions online are not of a harassing or predatory nature—indeed, they generally involve adults looking to help or assist minors in various ways. As the MacArthur Foundation study cited above concluded:

> In contexts of peer-based learning, adults . . . have an important role to play, though it is not the conventionally authoritative one. In friendship-driven practices, direct adult participation is often unwelcome, but in interest-driven groups we found a much stronger role for more experiences participants to play. Unlike instructors in formal educational settings, however, these adults are passionate hobbyists and creators, and youth see them as experienced peers, not as people who have authority over them. *These adults exert tremendous influence in setting communal norms and what educators might call "learning goals," though they do not have direct authority over newcomers.*[123]

A substantial portion of those interactions involve parents talking to their own kids, older and younger siblings communicating with one another, teachers and mentors talking to their students, or even co-workers of different ages communicating. Even when adult-minor communications involve complete strangers, there is typically a socially-beneficial purpose. Think of two people—one an adult and one a minor—debating politics on a discussion board, or creating a Wikipedia entry together. What about a Presidential campaign website that involves millions of volunteers of all ages communicating and collaborating to a common purpose? There are countless other examples. How would such interactions be affected by COPPA 2.0? Restricting such interactions would raise profound First Amendment concerns about freedom of speech as well as of association.

In any First Amendment analysis, a court must consider not only the free speech rights at stake and the availability of less restrictive alternatives to regulation, but the governmental interest being advanced. Again, neither COPPA nor the COPPA 2.0 proposals discussed herein (in New Jersey and Illinois) requires exclusion of older users from a website, nor directly governs the sharing of personal information among users (where that sharing does not also constitute collection by the site itself). But separation of adolescents from adults is likely to be an indirect effect of COPPA 2.0 requirements—as COPPA 2.0 advocates probably realize—because, once PI-collecting sites are required to age-verify users, they will face reputational, political and potentially legal pressure to make interactions between adolescents and children more difficult in the name of "child safety." More subtly, if PI-collecting site operators have an incentive to avoid being considered "directed at" adolescents, they will also have an incentive to discourage adolescent participation on their site—which achieves a similar result.

Here, one must further ask if attempting to quarantine children from adults (however indirectly) actually advances, on net, a strong governmental interest in child protection. Such a quarantine is unlikely to stop adults with truly nefarious intentions from communicating with minors, as systems designed to exclude participation by adults in a "kids-only" or "adolescents-only" area can be easily circumvented. Given the lack of strong identity records for minors, it's much easier for an adult

---

[119] *See supra* note 74.

[120] *SNWARA, supra* note 11, § 10(c).

[121] The original COPPA bill required that parents have "access to the personal information of the child of that parent collected by that website," S. 2326, *supra* note 14, § 3(a)(2)(iv)(I), while the bill as passed instead requires only that parents be given "*a description of the specific types* of personal information collected from the child by that operator," 15 U.S.C. § 6502(b)(1)(B)(I) (emphasis added).

[122] *See Mulligan Testimony, supra* note 118.

[123] *MacArthur Study, supra* note 117, at 39 (emphasis added).

to pretend to be a minor than vice versa. The effect of age stratification on truly bad actors is likely to be marginal at best—or harmful at worst: Building walls around adolescents through age-verification might actually make it easier for predators to target teens, since a predator who gains access to a supposedly teen-only site will be less likely to be exposed as a predator by targeting an adult they think is a teen. So for the sake of marginal (if any) gains in child protection, would we not be excluding beneficial interaction between adults and minors?

To hear some of the advocates of COPPA 2.0 talk about how teens currently behave online, one might think that online environments in which adolescents were left to their own devices—imagine a "Teen MySpace" for the 13–17 crowd, walled off from the rest of MySpace—would be far worse, perhaps an online version of *Lord of the Flies.* These concerns are clearly exaggerated: The critics frequently complain about "the way kids talk to each other these days" while looking at their own past adolescent banter with rose-colored lenses. What is clear is that adolescents (and young adults) behave better in online environments where adults are present, too. Perhaps the best demonstration of this fact has been the uproar from adolescents and young adults that has accompanied Facebook's explosive growth in popularity among older users in recent months.[124] Many kids hate the idea of adults joining Facebook precisely because the presence of adults encourages kids to "self-regulate" by exercising better judgment and following better netiquette.[125]

Anne Collier, founder and executive director of the child safety advocacy organization Net Family News, Inc. and editor of NetFamilyNews.org and ConnectSafely.org, suggests that the push for "segregation" by age (*e.g.,* creating a teen-only version of Second Life) for safety's sake is "losing steam" because:

> it's a response to the predator panic teens and parents have been subjected to in U.S. society, not to the realities of youth on the social Web. What nearly a decade of peer-reviewed academic research shows is that peer-to-peer behavior is the online risk that affects many more youth, the vast majority of online kids who are not already at-risk youth offline. Segregating teens from adults online doesn't address harassment, defamation, imposter profiles, cyberbullying, etc. It may help keep online predators away from kids (even though online predation, or abuse resulting from online communication, constitutes only 1 percent of overall child sexual exploitation . . .), which is a great outcome, but it's not enough unless all that parents are worried about is predators.[126]

Collier discusses the particularly acute problem of "actual or perceived sexual orientation and gender expression," which the *Salt Lake Tribune* has noted are "two of the top three reasons secondary school students said their peers were most often bullied at school."[127] This kind of harassment recently attracted widespread public attention after two 11-year-old boys committed suicide after experiencing anti-gay harassment and bullying at school.[128]

Nationwide, "Lesbian, gay, bisexual, transgender and questioning youth are up to four times more likely to attempt suicide than their heterosexual peers."[129] This child safety risk is painfully real, with anti-gay harassment being only its most obvi-

---

[124] Justin Smith, *Number of U.S. Facebook Users Over 35 Nearly Doubles in Last 60 Days,* Inside Facebook Blog Mar. 25, 2009, *www.insidefacebook.com/2009/03/25/number-of-us-facebook-users-over-35-nearly-doubles-inlast–60-days/*.

[125] *See, e.g.,* Lori Aratani, *When Mom or Dad Asks To Be a Facebook "'Friend," The Washington Post,* Mar. 9, 2008, *www.washingtonpost.com/wp-dyn/content/article/2008/03/08/AR2008030801034.html*. "'I do not know if this has happened to anybody, but this morning I log on to Facebook and I have a new friend request!' wrote 19-year-old Mike Yeamans, a sophomore at James Madison University, on one of several 'No Parents on Facebook' groups that have popped up on the site. 'I am excited to make a new friend so I click on the link. I could not believe what I saw. My father! This is an outrage!'" *Id.*

[126] Anne Collier, *Where Will OnlineTeens Go Next?,* May 1, 2009, *www.netfamilynews.org/2009/05/wherewill-online-teens-go-next.html* (internal citations omitted). For evidence of at-risk youth, Collier sites the *ISTTF Final Report, supra* note 8. Regarding the percentage of all child sexual exploitation that results from online communication, she cites Janis Wolak, David Finkelhor & Kimberly Mitchell, Crimes Against Children Research Center, *Trends in Arrests of Online Predators,* 2009) *www.unh.edu/ccrc/pdf/CV194.pdf; see also,* Anne Collier, *Major Update on Net predators: CACRC study,* March 31, 2009, *www.netfamilynews.org/2009/03/major-update-on-net-predators-mostly.html* (summarizing study).

[127] Anne Collier, *Anti-Gay Bullying Most Pervasive,* April 29, 2009, *www.netfamilynews.org/2009/04/anti-gaybullying-most-pervasive.html* (quoting Charles Robbins & Eliza Byard, *Gay Suicide: Addressing Harassment in Schools, Salt Lake Tribune,* April 24, 2009, *www.sltrib.com/opinion/ci__12220931* [hereinafter *Gay suicide*]).

[128] *Gay suicide, supra* note 127.

[129] *Id.*

ous form. But "segregating" teens from adults seems likely to aggravate this problem by removing adults from the mix as a potential source of discipline.

Of course, adults play a critical role in disciplining interaction among the 0–12 age bracket, but not as direct participants in on-site interaction. Again, how many adults actually want to use Club Penguin? Instead, parents can supervise what their kids do online through parental control software. Parents could, of course, use that same software to monitor what their adolescent kids do, too. But as kids get older, most parents realize that the training wheels have to come off at some point. Few parents will want to spy on their 17-year-old until the day before the kid starts college (or enlists in the military or gets married). But most parents probably would prefer that, if their kids are interacting in an online environment, they think twice about what they do and say online. It is by no means clear that restricting online interaction between teens and adults will serve that end.

VII. The Commerce Clause Implications of State-Level COPPA 2.0

State-based efforts to expand COPPA or to impose other forms of age/identity verification raise additional constitutional concerns: State-level efforts by state government or state AGs to push through an expansion of COPPA would likely violate the Commerce Clause of the U.S. Constitution.

For simplicity, the preceding discussion did not consider how PI-collecting sites would respond to COPPA obligations imposed in one U.S. state but not others. Sites might default to the "lowest common denominator" of whatever would be acceptable in the most restrictive states—especially if those states has populations as large as Illinois or New Jersey. But websites could also attempt to configure their services to function differently depending on what state the user is in. Thus, age verification mandates might also require location mandates (again, perversely requiring the collection of more information in the name of protecting adolescents' privacy). If a site relied only on location information provided by the user, adolescents would quickly learn to lie about what state they live in just as children have learned to lie about how old they are to avoid triggering COPPA's "actual knowledge" requirement. Alternatively, websites could attempt to determine a user's location automatically based on their IP address, but such "IP geocoding" is not always accurate and can be subverted by use of a proxy.

This technical discussion should help to illustrate why state-level COPPA 2.0 proposals would burden communication over the Internet, a uniquely "interstate" medium whose architecture makes it difficult, if not impossible, to isolate the effects of state regulation on residents of that state. There is a long string of "Dormant Commerce Clause" cases that have consistently struck down state laws attempting to regulate commerce (or speech) that originates or takes place outside the state's borders.[130] If it is not possible for a state government to isolate the effects of its regulatory actions to merely those PI-collecting site operators or users living within its jurisdiction, Federal courts will block such measures. Consequently, the extraterritorial impact of state-based COPPA expansion would likely result in an immediate constitutional challenge and such regulation would almost certainly be overturned.

It is also possible that COPPA 2.0 proposals may already be pre-empted by COPPA because, although COPPA authorizes state attorneys general to bring enforcement actions under certain circumstances,[131] COPPA bars states from enacting any laws "inconsistent" with COPPA.[132]

VIII. Summary of Implementational Challenges Regarding COPPA Expansion

Even if one somehow overcame the many policy and constitutional arguments against COPPA 2.0, there would remain a slew of difficult, if not impossible, challenges to overcome in implementing such a system. Most critically, the threshold practical question remains the same as it does for most other forms of online identity verification: *How do we verify the parent-child relationship when someone asserts they are the parent or guardian?* But there are many other questions regarding how well COPPA would "scale up" that must be considered:

---

[130] *See* Adam Thierer, *The Delicate Balance: federalism, Interstate Commerce, and Economic Freedom in the Technological Age* at 58–61 (The Heritage Foundation, 1999).

[131] 15 U.S.C. § 6504.

[132] "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 chapter that is inconsistent with the treatment of those activities or actions under this section." 15 U.S.C. § 6502(d).

1. *Verification Mechanisms.* What sort of mechanisms will need to be put in place to guarantee that the parent or guardian is who they claim to be (for both initial enrollment and subsequent visit authentication)? Sign-and-fax forms can be easily forged, so credit cards (and perhaps mandatory user fees) will likely become the default solution. A third method, follow-up phone calls, just doesn't seem practical. But might lawmakers demand a mix of all of the above?

2. *Obtaining Consent.* Regardless, how burdensome will those mandates be on parents or guardians? As Parry Aftab has noted, "The more difficult we make the consent mechanism, the fewer parents we will get to consent." [133]

3. *Costs to Business.* How burdensome will those mandates be for PI-collecting site operators? What kind of compliance costs or legal penalties are we talking about?

4. *Costs to Users.* Will those costs be passed on to users as fees beyond the nominal transactions required to achieve verification via credit cards? (Since most PI-collecting sites websites and almost all social networking sites are free-of-charge today, that's not going to be a very popular mandate!) [134]

5. *Disparate Socio-economic Effects.* How would increased fees or credit card mandates impact low-income families and youth, especially those without credit cards?

6. *Industry Consolidation.* If compliance costs—in the form of additional staff, insurance and litigation expenses—explode for website operators, will this cause the kind of industry consolidation that seems to have occurred with child-oriented websites since COPPA's adoption? Would the increased hassle of accessing new sites lead to consolidation by reducing adoption rates by users? How would online innovation and creative expression suffer as a result of such consolidation?

7. *Increased Privacy Risks.* Who would collect the massive data bases of information created by such a mandate? Who has access to all that new data? What might government use it for if they get their hands on it?

8. *Offshore Sites.* Could this new regime be applied effectively to offshore sites? Or, will kids flock to offshore sites as a result of such mandates on domestic sites? If some do, how will we stop them?

9. *Credential Transferring.* Even if the parental permission verification process worked during initial enrollment, how would it work in the "subsequent visit" stage? Once minors are given credentials or digital tokens, how do we prevent them from sharing or selling their credentials? In particular, how do we prevent older siblings from sharing their credentials with younger siblings? What would be the penalty for them doing so? What about older minors with independent access to credit cards?

10. *Law Enforcement Priorities.* How many law enforcement or regulatory agencies will be tasked with administering this regulatory regime? Might this be diverting resources from better priorities, such as serious law enforcement efforts and online safety educational programs?

IX. Conclusion

The future of age verification battles—at least on the social networking front—will likely be fundamentally tied up with COPPA and the question of how well parental consent-based forms of age verification might work on a scale larger than COPPA's very limited scale. It is unlikely, however, that such a framework could be easily applied on "Internet scale." There is a world of difference between a site like Disney's Club Penguin, for example, and sites like MySpace or Facebook. This ultimately reflects the uniquely insular nature of the under-13 age bracket and the lack of any clear line between adolescent-oriented and "general audience" content.

Moreover, as social networking capabilities become increasingly ubiquitous, integrated into every site and service—from *Change.gov* [135] to the *San Francisco Chronicle* (*sfgate.com*) to *CNN.com,* from Microsoft's Xbox Live service to Linden Labs' Second Life—the costs and hassles of compliance with COPPA 2.0 age verification mandates will increase dramatically. Are parents really going to be forced to authenticate themselves and then their kids for every website their kids want to par-

[133] *Aftab Comments, supra* note 59, at 5.

[134] Aftab also notes that "Parents do not trust a site to use their credit card to verify their consent. They barely trust online credit card use when they want to buy something." *Id.*

[135] Like many social networking sites, *Change.gov* allows users to comment on news items the IntenseDebate comment platform, which allows users to create profiles, upload profile photos, etc.

ticipate in that requires so much as an e-mail address? That mandate seems unnecessary and unworkable. Are other adults going to have to prove they're not adolescents? By creating such a requirement, COPPA 2.0 would also constitute a functional convergence of COPPA with COPA—a law the courts have rejected as inconsistent with America's tradition of anonymous speech, something central to our evolution as a democracy, pre-dating even the First Amendment that protects it from government interference.

Finally, the irony of COPPA 2.0 proposals is that lawmakers would be applying a law that was meant to protect the privacy and personal information of children to gather a great deal more information about them, their parents, and many other adults! These privacy implications should make us think twice about trying to expand COPPA beyond its primary purpose to encourage parental involvement in what kids do online. Even those who support COPPA in its current form should recognize that there are better ways to protect adolescents online.[136]

Related PFF Publications

- *Targeted Online Advertising: What's the Harm & Where Are We Heading?,* Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.
- *Parental Controls & Online Child Protection: A Survey of Tools and Methods,* Adam Thierer, Special Report, Version 3.1, Fall 2008.
- *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,* Adam Thierer, Progress on Point 14.5, March 21, 2007.
- *Social Networking Websites & Child Protection: Toward a Rational Dialogue,* Adam Thierer, Progress Snapshot 2.17, June 2006.
- *Age Verification for Social Networking Sites: Is It Possible? And Desirable?,* Adam Thierer, Progress on Point 14.8, March 23, 2007.
- *Is MySpace the Government's Space?,* Adam Thierer, Progress Snapshot 2.16, June 2006.
- *Rep. Bean's 'SAFER Net Act': An Education-Based Approach to Online Child Safety,* Adam Thierer, Progress on Point 14.3, Feb. 22, 2007.
- *Online Advertising & User Privacy: Principles to Guide the Debate,* Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.

The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties. Established in 1993, PFF is a private, non-profit, non-partisan research organization supported by tax-deductible donations from corporations, foundations and individuals. The views expressed here are those of the authors, and do not necessarily represent the views of PFF, its Board of Directors, officers or staff.

Senator PRYOR. Thank you.

I want to thank all the witnesses for their testimony.

And we're going to start off with Senator Rockefeller.

The CHAIRMAN. Thank you, Mr. Chairman.

I have this odd feeling about this panel, except you and you and you. It's like we're discussing some kind of—Is a breakfast cereal good for you, or not? And children have somehow already disappeared from this process. And it comes down, I think—I mean, and the both of you—Microsoft, Facebook—had good things to say, but you always ended up with the idea, "Well, we can—we'll do this by ourselves, and we really don't need the government telling us what to do."

And I have to leave, very shortly, because I have to give a speech on cybersecurity to a business group. Cybersecurity is the Nation's number-one national security threat, ahead of 9/11s, dirty bombs, weapons of mass destruction, according to all analysis. The private companies—this is very parallel to me—they always said, at the

[136] *See Parental Controls and Online Child Protection: A Survey of Tools and Methods, supra* note 17.

beginning, "We"—Olympia Snowe and I have been working on this for 2 years—"We can do this ourselves. We don't want government to be involved with this." We knew that couldn't happen, because we knew that they didn't have, really, any idea what they were doing about how to take on cybersecurity. Some of the larger companies did, to a certain extent, but, for the most part, they didn't.

That's like parents. We want parents to make these judgments, and which is a little bit like saying that some people here don't know how average American families have to live, where people are trying to keep down two jobs, and they, themselves, may not be skilled on the Internet, and in any event, they're tired, they have things to do. And so, we've got to do this for the parents. And so, "Well, let's not let FTC do this, let the Congress do that."

Well, maybe that was your idea, because you thought the Congress wouldn't be able to pass it. I thought your testimony was particularly unhelpful, to be honest with you. I thought both of your testimonies were terrific, because you were focused on the problem.

And, Mr. Rotenberg, or Dr. Montgomery—either one—we haven't, here, discussed, really, what the problem is. And the problem is, kids are watching filth. They're watching filth, and lascivious, horrible things, and we're trying to argue about 13, when, as you say, it should be 18 or 22, or whatever. And the companies, here, are in favor of cleaning this up, but not at the expense of being regulated. They want to do it themselves. They'd appreciate working with the FTC a little bit, but the clear message is, they want to do it themselves.

My clear message is, I don't really think they do. I think money trumps on this. Money always trumps when it comes to information. Money always trumps. This committee has come up with so many scam hearings in the last year or so. Money drives bad behavior, and then kids, or people, or whoever, or Internet users and popup—you know, all of these things are just left to the side.

So, I'd like you to describe, What damage do you think is being done to children by the inaction? And, you know, I agree with you some—agree with the FTC; they're not heavily staffed, they're not well funded. We need to change that. We're trying to protect them from being wiped out altogether under this financial services thing. And I think we have. I think we have done that. But, what is the damage that you see being done to a generation of kids coming up, with parents who are purportedly hovering over, watching every move they make, when you know perfectly well they're not?

Mr. ROTENBERG. Senator, I think the primary problem is that young people are being coaxed to reveal a great deal of intimate information. And the data is gathered and collected and disclosed to strangers, for any purpose that generates commercial value. And, as a parent of two teenagers, I have a problem with that. I think technology is great, and I want, you know, my kids to grow up and to be technologically literate and to make smart decisions online. Because I can't always be there, they need to have the tools and the experience to make those decisions for themselves. But, I know that there's a point where, if I can't help them and they can't figure it out, if the business practices are designed to conceal from them what's really going on. And that's why I think the Congress needs

to act. I think the Congress needs to give kids the ability to control how the information about them is being used by others.

The CHAIRMAN. My time is up. Do you have——

Dr. MONTGOMERY. Senator——

The CHAIRMAN.—one brief comment?

Dr. MONTGOMERY. Yes. I mean, I would agree with Marc. We have created—industry has created a system of ongoing monitoring and surveillance of teenagers, encouraging them. And it taps into their natural developmental needs to reach out to their peers and to become independent, encouraging them to give out a lot of information, and tracking everything they do, without their knowledge. It's also socializing them into a system where privacy is not valued. And I think that's a very deep loss to our society.

And then, finally, I do want to respond to what Mr. Szoka said about advertising. We're not talking about traditional advertising, here, by the way. We're talking about viral advertising and branded environments and interactive games and Avatars and a whole lot of things that are not what you traditionally think about as advertising.

And recent research has found that teenagers can be quite susceptible to this advertising; they're not necessarily aware of all of this, and we know they don't know what's being done behind the scenes.

The CHAIRMAN. I thank you both very much.

I thank you, Mr. Chairman.

Senator PRYOR. Thank you, Mr.——

Mr. HINTZE. Senator Rockefeller, could I make one brief comment, please?

The CHAIRMAN. Sure.

Mr. HINTZE. I just want to—I apologize if I gave the impression that Microsoft does not want government involvement, that we want to do this on our own. That's certainly not the case. We have been supportive, for a long time, of a multifaceted approach to protecting privacy online, not just for kids, but for all consumers, including our support for comprehensive Federal privacy legislation, which we think is essential.

But, self-regulation certainly plays a role. Industry best practices certainly play a role. But, education, law, regulation, and enforcement also play a role, as well, and we're very supportive of all of that.

The CHAIRMAN. I hear you.

Senator PRYOR. Thank you, Mr. Chairman.

Senator Wicker.

Senator WICKER. Well, thank you very much. And this is a very, very serious topic, with implications for the next generation. I appreciate the Chair's willingness to get into the weeds on this.

I do think that the testimony of all of our panelists has been helpful. I think it's important that we hear a variety of viewpoints, and all sides to this. And I do think that there's a way to—there must be a way to have it both ways, to encourage innovation and to protect the privacy of children's information at the same time.

So, I'll ask the panel, What do they think about what I just said? Has the law reduced innovation and caused consolidation among children's websites? Have we created a barrier to entry into the

children's website market? Has the law resulted in limitations on beneficial content specifically for children?

So, if we could just start with Ms. Rich and go down the panel, that'll be my question.

Ms. RICH. That's obviously—Tim keeps helping me with the button, here—that's obviously one of the key issues that we're going to look at in our review, especially since that was one of the goals of COPPA, is to preserve that access, even as kids were protected. We did review that issue that last time we reviewed COPPA, which was 2005, and we published a report. We sent a report to Congress, and we said, at that time, all of the commenters and all of the people we spoke to and the research we conducted indicated it had not, that children were being protected, and they still had access, and innovation was not being stifled. But, we are very interested in the answers to those questions today.

Mr. SPARAPANI. Senator, speaking only for Facebook, I can say that I have seen a strange disincentive because of the law. My whole testimony was focused on trying to identify all of the innovative things that Facebook has done for the teenaged users of our site. But, what you didn't hear me saying was that we're not spending a lot of energy on the under–13 set, because they're typically not on our site. But, there's a line that's drawn between the 13-and-over and the 13-and-under, and I think that that line has created a disincentive for companies to work toward innovating on the 13-and-under side. And I think that we need to look at that. And I think that's the point I was trying to make in my testimony, Senator.

Mr. HINTZE. I look forward to seeing what comes out of the FTC's current rule review. I can speak for our own company, that, yes, some of the parental consent mechanisms required under COPPA can be challenging, and sometimes frustrating to implement. But, I think that, for the most part, it has not discouraged us from continuing to provide services to general audiences, including young children and some specifically tailored to children, as well. It does create additional work and additional cost. It's a barrier to entry, in some cases, because anytime you're designing a sign-up process where there's a speed bump or even in some cases a significant barrier in having to involve the parent—yes, some consumers will go away and go elsewhere. But, we think it's in the—for the most part, the right thing to do. Involving the parent is the right thing to do. Creating those speed bumps so that you can inform children about the appropriate use of these services, and help educate their parents, is the right thing to do.

So, I would say, on the whole, COPPA has been successful in encouraging websites to do the right thing, even though there is a cost involved.

Dr. MONTGOMERY. One of the goals of the law was to minimize this massive data collection that was really becoming state-of-the-art in the early days of the dot-com boom and e-commerce. And I'm telling you, that is where the business was headed. So, what we were able to do—and, again, I repeat that we were worked with industry to come up with a set of principles that would honor the privacy rights of young people, but, at the same time, not interfere with the healthy development of e-commerce.

But, if you're going to market to kids, what we were able to establish is, there need to be some operating principles, here. And I think the industry has done a very good job of working that out. It was not easy to sit around the room and try to figure out, "OK, how do we do this?" You know, the parental verification mechanism was a tricky one, not easy to do. But, the idea was, first, enable the parents to know what their children are doing, and, second, make the industry aware that they have a responsibility, when they are collecting personal information from children.

We've seen a growth—a healthy growth of lots of wonderful websites for kids, lots of terrific content areas. And I think that has been a very, very good development, and I'm happy about it.

As I said, I think the 13 is not—kids don't become automatically mature at 13, as any parent can tell you. But, at that time, we decided, "Let's create this clear mark, here, for where we will have these guidelines." And now, I think we've seen a whole new development, with the web, that raises the issue about how—"OK, now what do we do about teens?" Again, not the same model, but, What can we do to ensure that they're treated fairly in this digital marketplace?

Mr. ROTENBERG. Thank you.

Senator I just want to say, I very much appreciate your question about the relationship between innovation and privacy. And I suspect we're going to hear a lot more about this.

But, if I could say, directly, sir, I think the relationship is not generally well understood. I don't see this as a tradeoff. My wife is a public schoolteacher. When we talk about innovation in the technology field and privacy, we think in terms of the privacy safeguards that enable children to take advantage of new technology. In other words, in the absence of privacy protection, I think you actually diminish the opportunity for technical literacy and training and education that parents and educators would like to see happen.

The real innovation that people are talking about, which is what they're not saying explicitly, is on the marketing side. They don't like the privacy rules, because they don't want to do the types of behavioral targeting, brand-based targeting, you know, "get your child to friend an advertising figure" targeting. That's the innovation they have in mind, and that's why they object to the privacy rules.

But, if we take a step back and talk about technical literacy, bringing more children to the online environment, creating great products and services so that they get excited about new technology, privacy actually plays a very big part in helping to make that happen.

Senator WICKER. Before we move to Mr. Szoka, let me follow up, Mr. Rotenberg. You mentioned that you have children. I take it that they are teenage?

Mr. ROTENBERG. Yes, sir.

Senator WICKER. Do you mind telling us how old they are?

Mr. ROTENBERG. Fifteen and sixteen.

Senator WICKER. OK. And I dare say that, in terms of knowledge about the protections that children need, you're probably in percentile 99.9——

Mr. ROTENBERG. Right.

Senator WICKER.—nationwide. That being the case, what do you need the government to do for your above-age–13 children, that it's not doing now?

Mr. ROTENBERG. I need the government——

Senator WICKER. Because you're a good parent.

Mr. ROTENBERG. Yes. Well, I appreciate that, sir. But, I need government to step in to control the things we can't control. In other words, if we sit down with our children and go through the privacy settings and say, "This makes sense," or, "This doesn't make sense," or, "That's really your call," and that's how we understand privacy protection, and then, the next week, the company says, "We've got a whole new approach now. We're going to do something different," and we're left with a sense that the tools that the company provided us to try to safeguard our privacy and the privacy of our children have basically become meaningless.

So, I—I'm not saying that parents don't play an important role. I think parents do. But, I'm saying it can't be made so difficult. And the businesses can't hide the way they collect and use data, as they do, because there's nothing that the user—the parent can do to change that. That's completely on the business side, and it's done because there is no regulation. There's nothing that prevents them from saying, to all the teenagers who they have data on right now, "You know, we've got a great idea, and we want to just go ahead and do this," or not tell them and go ahead and do it. Parents can't control that.

Senator WICKER. Thank you.

Mr. Szoka, you can respond to that, but also to the question about innovation versus privacy.

Mr. SZOKA. Well, thank you, Senator.

Let me be clear about three points.

First, there are always tradeoffs involved in regulation. And here, the tradeoff is not simply a question of economics versus privacy, but, indeed, the tradeoff involves free speech. And again, I stress that that's because "collection," as the term is used in COPPA, does not just apply to collection, as we mean it in the colloquial sense, such as is used for advertising or marketing purposes. But, under the statute, it's any sharing of information. It is the enabling of sharing of user-generated content.

So, when I talk, here, about the tradeoffs, I want to be very clear, I am talking about the ability of users to join tools, and the innovation in those tools that allow them to share and communicate and collaborate. And that's—this has been the flourishing of the Web 2.0. And that is exactly what is at stake here if COPPA were to be expanded in its age scope.

So, my second point is, I wanted to emphasize that I think one of the beauties of COPPA is that it gives the FTC great flexibility in shaping the rule within the confines given to it by Congress. So, the FTC has the flexibility to update the definitions of "personal information" and "Internet," and I encourage it to do so.

My caution, however, was that we ought to be very, very careful about having Congress reopen the door to the one thing that the FTC cannot, on its own, change, which is the age scope. And I mentioned the financial reform legislation only because that could, indeed, give a future FTC the ability to change things like the age

scope, which, again, presents an important tradeoff, in terms of free speech.

My final point is, there is a rich mosaic of parental control tools and software and methods available today. My colleague, Adam Thierer, at the Progress & Freedom Foundation, has published a comprehensive compendium of those tools. And again and again, in the context of filth, as Senator Rockefeller referred to, wanting to prevent or censor kids from accessing, the courts have repeatedly said that those tools need not be perfect, but the government regulation must yield to the tools, where they exist. And so, our point has been to highlight that these tools exist, and that we should be encouraging innovation, not just in the sharing of information, but also innovation in the controls that are available to parents, as well as all users, to take, really, control over their own information and how it's shared.

And so, our answer, in a nutshell, is that the solution to all these concerns should, first and foremost, be enforcement of the existing law, which applies to, again, children under 13, and then also education and empowerment. And government has a role to play, a very important one—and the FTC does this extremely well—in highlighting those tools, methods, and education. And I encourage it to do so, but, again, caution against changing the statute, itself.

Senator WICKER. Thank you.

Senator PRYOR. Thank you, Senator Wicker. Thank you for being here. And I know you have to slip out to another meeting, but thank you for your leadership. And we will leave the record open for a few days for Senators to submit their questions, if they want to.

Let me, again, thank all of our witnesses, but I want to thank Facebook and Microsoft for being here, because I know not everyone in the industry chose to come today. But, let me start, if I can, with a question for Facebook.

In your written testimony, you talk about "Facebook's culture of authentic identity." Could you elaborate on that a little bit?

Mr. SPARAPANI. Yes, Senator, and I'm glad that you asked.

One of the really interesting things that happened when Facebook was first launched is, we defied conventional wisdom at the time about privacy and security. We decided that, at the beginning, we were going to ask people to put their real names and build their entire profile around that. And I have to tell you, it has been the—really, the wellspring of a number of advantageous security and privacy benefits for users of all ages of our site.

Again, it was unconventional at the time, but what is meant is that we're able to really deter bad behavior; we're able to identify fake accounts quickly; we're able to target corrective action at an explicit account; and, more importantly, there's this community effect that takes place, where individuals feel some sort of reprobation when they take an action which is tied to their name. It tends to discourage bad speech, bullying, bad behavior, et cetera. And so, we've really been the beneficiary of this decision of, what we refer to as, a real-name culture.

Senator PRYOR. That's good.

And you also mentioned in your testimony that you didn't want to see any changes to COPPA.

Mr. SPARAPANI. We're not really needing changes at this point, because we feel we've done, really, a very good job of implementing the statute——

Senator PRYOR. Let me interrupt, right there.

Mr. SPARAPANI. Please.

Senator PRYOR. You're saying that's true for your company.

Mr. SPARAPANI. It is.

Senator PRYOR. Are you saying that's true industrywide? I mean, is everybody a good actor out there?

Mr. SPARAPANI. No, of course not. And, you know, there certainly are companies which are outliers, there always will be. And that's, frankly, why we need stepped-up FTC enforcement, to find those bad actors and take action.

Senator PRYOR. So, your view is, leave the statute as is, but beef up the enforcement?

Mr. SPARAPANI. Yes, I think that's the right approach, Senator. I think the FTC folks do a generally good job, and they would do better if they had more resources.

It's really easy to focus on the Microsofts and the Facebooks, the Googles, and the Apples, because we're here, and we can show up and testify. It's the companies that don't have people here in Washington, that don't have lawyers on staff, that probably deserve the lion's share of attention; they don't get it, because the press can't focus on them, and they can't be found.

Senator PRYOR. Tell me why you like the age 13, and why you think that shouldn't change.

Mr. SPARAPANI. Well——

Senator PRYOR. My, just general inclination would be, "Hey, this is a children's issue, you should make it, 18 and under," or, something like that, move it up a few years. But, tell me why you like 13.

Mr. SPARAPANI. Well, first of all, Senator, my expertise is in privacy, and it's not really in child psychology or social development. So, I can only speak from this perspective. We have found that teenaged users have really had a, really, very successful experience on Facebook. They're socialized well, they learn good rules of behavior, they are able to actually advance themselves and learn about the world around them.

So, what—I would not want to see us deny teenagers the opportunities of living in a digital society. I think it would hamper kids around our country, and set them back, vis-á-vis children of the same age in other countries, if we were able—if we were to prevent them from having access to these sites or services.

Senator PRYOR. OK.

I think—Dr. Montgomery, did you have a comment on that?

Dr. MONTGOMERY. Yes. And I would agree that social networks, and the Internet in general, are terrific tools for young people. I'm also the mother of a teenager, and I can see what a great role these new digital technologies are playing in her life, and they really do tap into the key developmental tasks of adolescence, when adolescents are exploring their identities and they're trying to reach out to their peers and really separate from their parents, which is something that they need to do, and be more autonomous. So, I can

really see that. And a number of my colleagues have done terrific research that documents all of that; I think that's great.

And I—but, I think the problem is that teens are out there in very public and very transparent—in many ways that sometimes alarms parents, on these social networks. But, the business practices of data collection and surveillance that's taking place on Facebook and other social networks is not transparent. It is really a black box, in many ways.

And I would not be talking about restricting teens from having access to these platforms. I think we need to give them that access; they're very important. But, I—what I would be calling for, and what I do call for, is for the government to play a role in ensuring that all of these social networks, and all of the platforms, mobile and otherwise, that young people are engaged in, are operating by a set of rules. These rules can be crafted in a way that will balance free speech, that will balance business and innovation.

When we started talking about COPPA, a lot of people said, "Well, we'll never be able to do this, this is impossible." We were able to work it out. And again, not the model that we have for COPPA, not the model of parental verification and restricting access, but a separate set of principles that I think we could work out together that would apply to teenagers.

Senator PRYOR. Let me ask you, Dr. Montgomery, are there a set of principles that exist right now? Is there a model rule out there that we could apply here? Or do we have to start this from scratch?

Dr. MONTGOMERY. Well, I think at the very least, the—some of the international principles—OECD principles, for example, that Marc can talk to about data minimization and transparency and other things that we would expect—you know, I don't see a model out there, as yet. I think we're inventing some of these things, as we did with COPPA, but I think this is the right moment to do so.

Senator PRYOR. And while I'm on you, Dr. Montgomery, should we leave age 13 as is, or should we change it?

Dr. MONTGOMERY. I think COPPA operates well as it is. I'm not necessarily talking about revisiting the actual legislation, but I do think we ought to think about what protections we could provide for teens. And again, I think we need to be careful about the model that we create, that I don't want to see teens totally ignored.

Senator PRYOR. OK, Mr. Sparapani, let me ask you, you all apparently have a "report" button. And how often is that used? I mean, do you track that? What are the numbers on that?

Mr. SPARAPANI. Well, Senator, I don't have the numbers, here, immediately in front of me. But, I have to tell you, it's enough to keep a huge team of employees busy, all day, day and night, from around the world. When you have 400 million users, which we do, and they're trained, because they've become comfortable with self-reporting, what they consider to be inappropriate behavior by others on the site, it does produce a large quantum of reports.

And, of course, we triage those. We take the ones that might have a law enforcement component, we put those at the top of the list, in terms of responding. We put the ones that concern potential threats to life and limb—and it only happens rarely—but, we put those, and we prioritize those. And so, these other reports about

other malicious behavior or inappropriate speech drop down a certain notch.

Senator PRYOR. And does your company have policies that go beyond COPPA? I mean, it sounds like you all have a set of policies that really go beyond the law.

Mr. SPARAPANI. Well, I guess the one place where I would suggest this is in—with respect to our marketing practices. I want to distinguish Facebook from virtually all other companies I know, and from some of the generalized discussion that has been happening about marketing to teenagers.

With respect to marketing to teenagers, Facebook never, ever shares information with the advertiser about individual users; doesn't matter the age of the user. What we do is, when we get a request to advertise on our site by a company, we offer the ad, but we never share the actual personal identifiable information with that advertising company. And I think it's important that people recognize——

Senator PRYOR. You give them aggregate information about your users, but not specific information?

Mr. SPARAPANI. That's exactly right. I think it's an important protection. And I think it has really helped our company succeed. And I hope other companies will follow our lead on that.

Senator PRYOR. Mr. Hintze, let me ask you, I know that Microsoft, through, you know, your various software products, offers a lot of parental controls. Do you know what percentage of your users actually utilize the parental controls? Do you have a sense of—even a kind of rough percentage of what that might be?

Mr. HINTZE. Yes, I don't have the actual numbers with me, and I think it probably depends on the service itself.

Things like Xbox Live, for example, the parental controls are really built in as part of the account creation process. So, when a parent buys an Xbox and signs up for an Xbox Live subscription, part of that transaction of creating secondary accounts for their children put those parental-controls choices in front of the user. So, it's quite a high percentage of users who are children, where their parents are utilizing those controls to some level. And there are all kinds of different knobs and dials in there; and how deep the parents go probably depends on the parent. But, a large percentage of users are using that.

Other services, you know, we've got this Windows Live Family Safety, which is a free download for people to use to help control how kids are surfing the Net and using search services.

You know, there's a challenge of educating parents and making them aware of these tools, and it's something that we try to do, but it's always hard to reach those parents. One of the reasons why we have implemented parental consent processes, even in cases where we think COPPA doesn't explicitly require it because it's a general audience site, for example, we think that's an opportunity to provide that kind of education to parents, to get some of these tools and information in front of them.

So, it really depends across the service, I think.

Senator PRYOR. Let me ask about your—you call it Windows Live Family Safety?

Mr. HINTZE. Yes.

Senator PRYOR. Let me ask about that product. That's free?

Mr. HINTZE. Yes, it is.

Senator PRYOR. And how do parents find out about that?

Mr. HINTZE. We provide messaging in a variety of different ways. We have worked with a number of organizations—children's organizations—to provide information through those, the Boys and Girls Clubs and other organizations like that. We've provided information through our own sites; we've got dedicated Web pages around privacy and children's safety on our websites to provide information to parents. So, there are a variety of means about how we try to get, sort of, the word out on these different tools that are available to parents, get them educated about the risks of children online and the risks that those children face and the tools available to them, to help protect them.

Senator PRYOR. Yes, I think it would be helpful for parents—and you may already be doing this, I'm just not aware of it with this product—but, I think it would be helpful for parents if you guys could take the offensive and aggressively, periodically, from time to time, whatever's appropriate, offer almost like a parent's toolkit on how to stay safe online.

And there are a lot of aspects of that. I mean, there's identity theft; there are a lot of fraud issues; there are just privacy issues with kids or with—I mean, you know, just really kind of runs of the gamut. And does Microsoft offer that, kind of in one place, these kind of, you know, semi-regular reminders that these tools are available, and, "You need to update your settings," et cetera, et cetera? Do you all do that, or is that not——

Mr. HINTZE. We do have——

Senator PRYOR.—proper etiquette——

Mr. HINTZE. Yes.

Senator PRYOR.—you know, in your company?

Mr. HINTZE. We do have the equivalent of tool kits available. We've got a website that has a list of resources available to parents, and information available to them, to help educate themselves and their children about the risks online. Again, the challenge is making them aware of that. And——

Senator PRYOR. Yes.

Mr. HINTZE.—and there are certainly things that we have done in the past, sort of, quasi-marketing campaigns to parents, to try to get that information in front of them. And there's obviously more we can do in the future.

Senator PRYOR. Yes, I'm not a—personally, I'm not a huge Internet user. I mean, I use it probably every day, but not extensively every day, and usually not very extensively at all, but, you know, I wasn't aware of that. So, if I'm kind of like Average John Q. Parent, here, I didn't know that was out there. So, I would hope that Microsoft and other companies would think about ways to be a little more aggressive in letting people know.

Let me go ahead and ask Mr. Szoka about the age 13. You want to keep 13 where it is?

Mr. SZOKA. Senator, yes, I think you've asked the most important question of the day. The point that I've tried to raise is—this is perhaps the least well understood aspect of COPPA. And the point, here, is not necessarily just to deal with child psychology, although

13 does happen to be the age at which Jewish kids are Bat Mitzvahed, the Confirmation is given in the Catholic Church. Romeo and Juliet were 13. There are reasons why 13, historically, has been an age of transition and, indeed, was chosen by Congress.

But, the point that we've tried to stress in our work at PFF has been that the far more important reason for keeping it at 13 is that, when you raise that age above 13, the COPPA framework breaks down. Because, again, as I said, COPPA basically applies, in two ways: It applies to sites that are required to presume that all of their users might be a child, and then again where sites have actual knowledge. And so, if you were to set that at 18, for example, you would end up in a situation where sites that were—that might be considered directed at adolescents, or might be afraid that the FTC would find them to be so, are sites that differ profoundly from sites that are, today, like Club Penguin, really, truly directed only at kids under 13. And the difference is, adults use those sites that teens use, as well.

And so, as a practical matter, if you extended the COPPA framework to a higher age, you would, for the first time, have the government be requiring age verification of large numbers of adult users. And we've already been down that road before. The courts have very clearly held, in the litigation about the Child Online Protection Act, or COPA, that to do so would be unconstitutional because it would infringe on the free speech rights of users to access content without having to identify themselves, such as through use of a credit card, but also the free speech rights of the sites themselves, to reach an audience, which is diminished by the roadblock of age verification.

So, I want to be clear that, from my perspective, this is the most important issue that we've talked about here today, understanding why that age for COPPA must be kept at 13 for the framework of the—of what I think is a really great statute, otherwise, to function effectively.

Senator PRYOR. Thank you.

Mr. Rotenberg, do you agree that COPPA breaks down if you change the 13-year-old threshold?

Mr. ROTENBERG. Yes, I've been sitting here, listening to Mr. Szoka's comments, and I'm just very confused. I actually helped litigate against the COPA, which was the Act that raised the First Amendment concerns. And on that side, he and I are actually on the same page.

But, it is almost completely unrelated to the discussion we're having about age verification and COPPA. As Mr. Sparapani explained, every person of any age who wants a Facebook account has to, in the first instance, provide information about their actual date of birth; that's how they make the determination whether someone's above 13 or below 13. And presumably, they could do the exact same line drawing exercise at age 18. So, this argument actually doesn't make any sense to me.

But, what I—what Mr. Sparapani said, which I think is something that needs to be considered more carefully—and I understand where he's coming from—he said, basically, Facebook made a decision, for children under 13, "We just don't want to have them as users." In other words, "It's too complicated; and because of the

COPPA obligations, we're just going to say, you know, 'Wait a few years,' basically." And he suggested, in his answer, that if Congress were to extend the line to 18, perhaps they would make the same decision now for kids between the ages of 13 and 18, which is obviously not what we're suggesting. We're not saying that teenagers shouldn't be on social network services. We're saying that companies that provide social network services to teenagers should have some legal restrictions on the collection and use of data about those children. And I think that can be done without too much difficulty. It would probably be based on COPPA; you probably want to make some changes.

But, that's the main legislative recommendation I would make: create some legal protections for teenagers. Don't discourage them; I agree with others, it's a good service. But, as it is right now, it's not providing adequate protection.

Senator PRYOR. Let me ask about age verification. I know some companies may differ with me on this, but my impression is that there's really not a way that exists, yet, to truly get rock-solid age verification. And filling in your birthday—obviously, kids can just put in a different date and, you know, they may be off to the races. So, am I wrong on that? Is—that there's not a really good, solid way to do age verification yet? Or, tell me—tell me what—the state-of-the-art right now.

Mr. ROTENBERG. Well, it has always been a challenge. And I think you're exactly right to say that there is no, you know, rock-solid way to do it. There are a number of different techniques. Facebook itself, I think, has developed some pretty good systems to do age verification. I think they probably get it right at a very high level, which is to say, I would be very surprised if there were a large number of accounts for kids under 13. There may be some out there; I suspect that's true. But, I don't think it's a very large number.

And I think a similar, you know, effort to move the age line to 18, there will probably be some people who get, you know, in under. But, I don't think that's a reason not to do it. And I think it would be a mistake, actually, to say, "Well, because we can't get it, you know, 100 percent, we should just give up."

Senator PRYOR. Right.

Mr. Szoka.

Mr. SZOKA. Senator, if I may respond, you are exactly right that there is no perfect method of age verification. But, there is another important distinction we have to understand, here. And it's as simple as the fact that when you sign up for a site, like Facebook, today you are indeed, as Marc has mentioned, required to provide your age. But, you can, indeed, Senator, as you have mentioned, simply lie. And the critical difference here is, that as it—as these sites function today, sites like Facebook and the many other sites—because this is not just about Facebook, but indeed about every site that potentially allows sharing and posting of comments, such as the blog that I run, for example—that when you sign up for those sites, you are not required to verify your age through the use of a credit card. This is the key issue.

My point here is that, if we were to move to a world where COPPA applied to children under 18, you would have large num-

bers of sites that enable the sharing of—by users, of information about themselves—so-called user-generated content—to have to actually age-verify. And that's a fundamental difference from the current regime in which sites simply ask for age, and if you admit that you're under a certain age, they block you, as they're required to do. And it's at that point that you start to run into precisely the same constitutional issues as were raised in COPA. Because COPA, in a nutshell, required certain sites to assume, again, that all their users might be children, and therefore require all users to verify themselves with a credit card, or similar tool.

Senator PRYOR. Dr. Montgomery, let me ask you about the state of academia on this. And that is, Are there studies out there, where people have really analyzed, maybe the child psychology or, how the industry really operates? I mean, is there a body of academic work on this that the Subcommittee can look at to, you know, get some insights on how things really work out there?

Dr. MONTGOMERY. Well, there's a growing body of research about how young people are interacting with online social networks and other digital media; the MacArthur Foundation has funded a good deal of work in that area. None of it, I have to say, has really taken into account, or looked at, the commercial dimensions of the digital media.

Senator PRYOR. And privacy doesn't——

Dr. MONTGOMERY. Or the privacy.

Senator PRYOR. Yes.

Dr. MONTGOMERY. Now, there are some studies emerging on privacy, but they're not looking at the whole picture of digital marketing.

I will say, also, that the experts in the food marketing area—and I'm working very closely with a number of them—because of the concerns about childhood obesity and the role of food marketing in that crisis, have begun to pay more attention to the digital marketplace. And I've been doing a lot of research in that area and am working with experts who are looking at adolescent development and the role of adolescents in the digital marketplace, because they're very much at risk for childhood obesity, and they're not necessarily in a position to be asking their parents about their decisions about food.

And we know that many of those food marketers are using behavioral targeting and behavioral profiling to target, in interactive games and in other kinds of online settings, precisely those kids who may be most vulnerable to that kind of marketing.

So, we are working with a number of people to conduct more research in that area. I'd be happy to supply the Committee with some of that research.

Senator PRYOR. Yes, I'd like to see that.

And so, when you're talking about, say, fast-food marketing, give me a scenario where that works. It sounds like, to me, that some kid may be walking down the street, and there's a fast-food restaurant, and he may get a message on his or her phone that they should go in there, they get a coupon or something. I mean, tell me how that works.

Dr. MONTGOMERY. That is where location marketing is going. And that is—you know, first of all, you know who the individual

consumer is. And as we're finding, you know, it isn't always necessary to even know the name. You simply know—need to know who that person is who is using that particular mobile phone, and, you know, what the age is, and the other demographic characteristics, as well as the behavioral characteristics—what kinds of sites they go to, and masses of amount of data that are being pulled together by various tracking technologies.

And, yes, the idea—and we've seen some trials with this, with some of the fast-food companies—would be, you know, that you're—when you're near that restaurant, you would get a coupon that could say, you know, "You can get a discount for this particular kind of product."

We're also looking at interactive games and the kinds of behavioral profiling and targeting that's going on there. So, let's say you're a pizza lover, you're also addicted to interactive games, and interactive games online can then target you when you're most, you know, aroused by the game and offer you pizza, and even provide you with direct access to an online site to order that pizza. And we know of—also, that we're looking—a lot of apps on phones—I have an iPhone—that enable you to order things right away. So, it's this kind of impulse buying. All of that is tied into behavioral targeting.

Senator PRYOR. And so, let me ask a follow-up there. You mentioned the iPhone, which is an Apple product; so you have the manufacturer of the phone, but you also—what about the wireless companies? The cell phone companies themselves, the AT&Ts and Verizons of the world? Are they providing this type of information to marketers? I mean, are they giving age and things like that? Do we know that?

Dr. MONTGOMERY. It's my——

Senator PRYOR. Has anybody looked at that, that we know of?

Dr. MONTGOMERY. Yes, I mean, Marc, you may be able to answer that better, but they fall under a certain set of policies——

Senator PRYOR. Right.

Dr. MONTGOMERY.—you know, that are—that apply to those companies, that are——

Senator PRYOR. Right.

Dr. MONTGOMERY.—separate from what some of the online companies would.

Do you want to answer that one?

Senator PRYOR. Do you know?

Mr. ROTENBERG. We're not specifically aware of how the telephone companies collect the data on customers. But, there was a very interesting proposal to do a so-called "deep packet inspection" by Internet service providers which would actually reach much more deeply into the personal activity of people online, literally looking at all the e-mail traffic they were sending, and trying to take, you know, pointers to commercial activity out of that.

I do want to make, just on this point, one further comment. I think Mr. Sparapani was correct when he said, earlier, that Facebook doesn't disclose user data to advertisers. That's right. But, Facebook does disclose user data to application developers so that when a Facebook user installs a Facebook app—you know, favorite cities or snowball fight, or whatever it is—Facebook, at that point, is making a decision to send a lot of the user's social graph

over to that company. And what they announced, just recently, is to do something very similar with third-party websites, like CNN and Pandora.

So, it's not the whole story, I think, at least in this situation, to say, in terms of Facebook, that the data doesn't go to advertisers. There are other ways that the data is released.

Senator PRYOR. Thank you.

And, Ms. Rich, I haven't forgotten about you.

Ms. RICH. I'm listening, here.

[Laughter.]

Senator PRYOR. Let me ask you a few questions. First, did you have any follow-ups on any of this that you heard that you wanted to clarify?

Ms. RICH. Well, I do have one follow-up from something Marc Rotenberg said, in his first statement, which is, I agree wholeheartedly that enforcement by the FTC, both of COPPA and generally in privacy, is very important. And we are very proud of our enforcement record. Just in the last year, or even 6 months, we brought four data-security cases, which puts us at close to 30 data-security cases that we've brought. We've issued an Online Behavioral Advertising Report, and done at least one case involving deceptive tracking. We've done eight cases designed to promote the integrity of self-regulation. And I could go on and provide the—provide you, Mr. Chairman, with more. But, I did want to comment on that.

Senator PRYOR. Yes.

In your statement, you said—let me—I think I have this right—whether the rule's definitions of "Internet" adequately encompasses certain technologies, like mobile communications. I don't know if you remember that. And is the FTC looking at what we even mean by "Internet" today, and—the definition of "Internet" and "mobile technology"? I mean, are you reevaluating all of that, in light of the technological innovations?

Ms. RICH. Yes, the—there was the standard definition that was very sci-fi-sounding, back—that they were using in all of the statutes when COPPA was passed, you know, "the World Wide, you know, Infrastructure," and—you know, it's a strange definition. And it's not clear whether that encompasses just traditional online activities or whether it would extend to interactive activities that don't actually go through the Internet. So, we're very—looking at that very seriously.

Senator PRYOR. Knowing what you know now, in terms of the state of technology, but also what FTC has to deal with, with the statute, and looking at the statute, would you recommend that the Senate revisit some of those definitions in the underlying law right now?

Ms. RICH. Well, we're taking a hard look at that, and in a few months we'll have the benefit of, hopefully, many, many comments on it. And at that point, we'll figure out what our next move is, whether it's something we can address, or not address, in the rule—meaning, we have the authority under the statute—or whether it's something we'd have to come back to Congress on.

Senator PRYOR. OK.

You know, one of my staff guys, here, just gave me a little device that's a Nintendo DS, which is interesting. I don't know if it's his or his child's, but it has a Pokeman attached to it, so——

[Laughter.]

Senator PRYOR. Anyway, but it has a phone on it, and I don't know if it plays music or exactly what. But, you know, obviously it's a little game; it has a little game cartridge in there. But, it also, very easily and very quickly, allows the child to connect to the Internet. And, you know, it has the camera, you can do shopping and that type of thing. So, you know, this is a device that obviously didn't exist, just a few years ago. And I guess I would encourage FTC, as you're looking at this, to think through all the applications and—maybe not, you know, the—I think it's probably hard to make a list of all of the devices, but just the functionality of it. If it's connecting to the Internet, and if it's mobile and things like that—because hopefully the electronics industry will continue to innovate, and will continue to do great things, and bring things on the market, and, you know, hopefully when the FTC goes through your process, you'll define things in such a way, and you'll work with us to define things in such a way, that when new products like this come onto the market, you know, the statute captures that and we don't get out of date.

I——

Ms. RICH. Can I just say——

Senator PRYOR. Yes, please.

Ms. RICH.—that we have two of those in our house; one for my 12-year-old and one for my 9-year-old, and they——

Senator PRYOR. So, they're——

Ms. RICH.—talk to each other. And when it does access the Internet, I think we would be safe to say that's covered, because it's accessing the Internet.

Senator PRYOR. Right.

Ms. RICH. But the question is, if they're just speaking to each other, and not through the Internet—there's functionality that just can go, you know, machine to machine.

Senator PRYOR. Right.

Ms. RICH. Is that covered?

Senator PRYOR. Right.

Well, it is just an example of things that I know the Federal Trade Commission has to think through.

I could, actually, spend a lot more time asking questions, because this is very interesting. And I know that we've had—our members here had to move on to either speaking on the floor or other committee meetings they had to get to.

So, let me just do this, at this point, let me just ask the panel if there's anything anyone would like to say before we close down the hearing, because we've had a little bit of back-and-forth, and I just wanted to give everybody a chance to respond or to make one last final point.

So, is there anybody that wants to add anything?

Mr. ROTENBERG. Very briefly, Mr. Chairman, I just wanted to thank you for holding this hearing. I mean, I think there are a lot of people who appreciate COPPA and believe it plays an important role in safeguarding online privacy, but also feel that, given new

technologies and new business practices, something more probably needs to be done. So, this is a very good place to start that discussion.

Senator PRYOR. Thank you.

Mr. SZOKA. Sir, if I may say, just briefly, I wanted to stress in my testimony that COPPA is device-neutral. And that's one of the great things about the statute. The example you gave, I think, Ms. Rich, is exactly right, here. We may not need changes to the statute, the FTC will look at that, but I think that the FTC probably has the flexibility to apply "the Internet" very broadly to all of those services that touch upon, and are integrated into, the Internet.

So, again, I want to stress, here, my concerns are not with the FTC updating the rules consistent with the statute, but simply about making broad changes to the statute that have greater consequences for speech.

Senator PRYOR. OK, thank you.

Yes, ma'am.

Dr. MONTGOMERY. Yes, I again thank the Committee for holding this hearing. It's very heartening for me to hear, having struggled with many others in the 1990s to get this law passed, that it has been a success. And I'm very pleased about that, and I'm very pleased to be working with the FTC to ensure that COPPA is able to address the continuing rapid changes in the digital marketplace.

But, again, I would just like to make a plea that we, as a society, and that the government and the industry, not ignore the needs of the Nation's teenagers.

Senator PRYOR. Right.

Mr. HINTZE. I'd, again, like to thank you for holding this hearing today, and the members of the Committee for participating.

A lot of discussion today around kids, and a lot of discussion today around teens and the ages not covered, currently, by COPPA. I think our position, and a number of the other panelists, is that COPPA may not be the right vehicle to address the teen issues. The issues that teens face online are somewhat different from those that younger children face, the types of sites they use are quite different, in many cases. But, others have expressed the need for some legal protections of teens, and we agree. And so, we would encourage the Committee to continue to look at the privacy issue more generally, maybe not in the framework of COPPA, but looking at privacy legislation, at the Federal level, that would address privacy protections for not only teens, but adults, as well.

Senator PRYOR. Good.

Yes, sir.

Mr. SPARAPANI. What's new from our perspective, since the dawn of COPPA, is that we're entering a moment, I think, in the Information Age, for the first time, when we actually have the opportunity for technology to reinstill privacy into people's online lives through new tools. And there's this sort of user-control model that Facebook and a number of our—companies like us are trying to put forward, is a really new thing, and it actually holds real promise for user privacy.

What's more difficult is getting users to understand the new tools and use them in a wise manner, and to, frankly, find them and ex-

ercise them. And it's especially hard with teenagers. So, that's someplace there where I think we're going to spend some energy.

But, again, thank you, Senator, for holding this hearing.

Senator PRYOR. Thank you.

Ms. RICH. And I'll echo the thanks to you, Mr. Chairman, and to the other panelists, for engaging on these important issues.

And also say that we should have a lot more to report after our comment period closes and after we have our workshop in June. So, I look forward to talking some more.

Senator PRYOR. Thank you, Ms. Rich.

Let me ask the FTC one last question, and that is, As part of your evaluation are you also looking at your manpower, slash, resources there at the Commission? I mean, some of the witnesses have said that if you had more resources, you could do more enforcement and be more effective in enforcing COPPA. Are you all evaluating that, as well?

Ms. RICH. Yes, we are.

Senator PRYOR. And will you come back to the Senate with a recommendation on that?

Ms. RICH. Sure.

Senator PRYOR. OK. Thank you very much.

[Laughter.]

Senator PRYOR. And I guess, in closing, I'd like to say, we're going to leave the record open for 2 weeks. So, don't be surprised if some of the Senators or the staff here want to submit some more questions, because there are some I didn't go into because I've taken too much of your time already. But, we'll probably submit some of these over the next couple of weeks. We would ask you to get those back as quickly as you can, and always work with our staff.

But, in closing, I'd like to say, this may be one of those areas that I think that Senator Wicker kind of alluded to earlier. There's an old Abraham Lincoln quote that says, "Government should do for people what people can't do for themselves." And this is an area where we want people participating in the marketplace, and using this technology, and enhancing their lives, and doing all of these great things. But, we just have to make sure that that marketplace is secure, that the right privacy parameters are there, the right legal structure is there, we have the right enforcement. I mean, we just have to make sure that that marketplace is working, because the people can't do this for themselves. I think there's a level of government, and certainly private sector, the private industry has a lot of good actors in it, but there are some bad actors, as well. So, we're trying to find that balance.

But, anyway, thank you all for your participation today. I know Chairman Rockefeller appreciates it, and I do, too, and all the Subcommittee.

So, thank you very much.

And, with that, we'll adjourn the meeting.

Thank you.

[Whereupon, at 11:52 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO JESSICA RICH

Question 1. Do you think the age limit in COPPA is appropriate? And if so, why?

Answer. After looking closely at whether adolescents should be covered for purposes of the COPPA statute, Congress chose to define a "child" as an individual under age 13. This choice was based in part on the sense that most young children do not possess the level of knowledge or judgment to determine whether to divulge personal information over the Internet. The FTC supported this assessment at the time the COPPA statute was introduced.* The staff anticipates it will receive comments on this issue during the FTC's COPPA Rule review.

Question 2. Do you think COPPA should be strengthened?

Answer. The FTC currently is reviewing the COPPA Rule in its entirety in light of significant changes in the online environment, including the rise of social networking and the proliferation of interactive technologies, and the increasing use of the mobile web and interactive gaming. Through the FTC's March 2010 request for written public comment, as well as its June 2 roundtable, the agency intends to explore what's working optimally, and where changes might be warranted. Once we have completed the public roundtable and the comment period has closed, the Commission will carefully evaluate whether any modifications to the Rule are warranted.

Question 3. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

Answer. The FTC is reexamining whether the Rule's current definition of "personal information" needs to be revised, consistent with the COPPA statute (*i.e.,* permitting the physical or online contacting of a specific individual), to include, for example, other types of information such as user or screen names and/or passwords, zip code, date of birth, gender, persistent IP addresses, mobile geo-location information, or information collected in connection with online behavioral advertising. The FTC has asked for written comments on this issue and the FTC staff has dedicated a panel at the June 2 COPPA roundtable to the question (see agenda, at *http://www.ftc.gov/bcp/workshops/coppa/Agenda_2010COPPARoundtable.pdf*). At this time, it would be premature to conclude whether the FTC is likely to amend the Rule's current definition of personal information.

Question 4. In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

Answer. For many young people, socializing and communicating online can be a rewarding experience, but those activities come with risks, including:

- Inappropriate conduct, including online harassment, cyberbullying, and sexting. The online world can feel anonymous. Young people sometime forget that they are still accountable for their actions and do not realize that they may lose the ability to control the dissemination of information and photos once they are shared online.
- Inappropriate contact. Some people online have bad intentions, including bullies, predators, hackers, and scammers.
- Inappropriate content. Young people may find pornography, violence, or hate speech online.

---

*See September 23, 1998 Testimony of the Federal Trade Commission before the Subcommittee on Communications, Senate Committee on Commerce, Science, and Transportation, available at *http://www.ftc.gov/os/1998/09/priva998.htm*.

It is difficult to determine what the "biggest threat" might be, because every child has unique circumstances that affect his or her personal risk profile. The FTC is closely following research conducted by the Pew Internet & American Life Project and the Crimes Against Children Research Center, among others, so that we may better understand the interplay between children's experiences and the risks they face online. Such research helps us craft useful advice for parents and children, such as the advice for parents in our recent publication, *Net Cetera: Chatting with Kids About Being Online*.

Question 5. What do you think is the most urgent update to COPPA needed?

Answer. As stated above, the FTC currently is reviewing the COPPA Rule in its entirety. Through the FTC's Rule review process, the agency intends to take a careful and comprehensive look at the Rule, with input from many sources. The agency is keeping an open mind, therefore, on what the most pressing modifications, if any, might be to the Commission's Rule or to the underlying statute.

Question 6. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

Answer. The COPPA statute does not define or use the term "sensitive data." However, the statute does contain an enumeration of what type of individually identifiable information is considered to be "personal," the collection of which requires an operator to obtain prior verifiable parental consent. "Personal information" is defined as:

> 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.

In promulgating the COPPA Rule in 1999, the FTC used the open-ended authority granted under subpart F of the definition of personal information to add "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." The Commission also added to the definition "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." Since promulgating the COPPA Rule, the FTC has not further expanded upon the definition of personal information. However, as noted in our response to the previous question, the FTC is reexamining the definition of "personal information" as part of its overall Rule review.

Question 7. You mentioned major tenets of children's privacy the FTC will consider in its reexamination of the effectiveness of COPPA. Specifically, you address "whether the Rule's definition of 'Internet' adequately encompasses [certain] technologies" like mobile communications. Will the FTC consider in its review the impact of data and location tracking devices, such as GPS systems, on children's safety?

Answer. Yes. The FTC's March 2010 request for public comment seeks input on whether the Rule's current definition of personal information needs to be revised, consistent with the COPPA statute *(i.e.*, permitting the physical or online contacting of a specific individual), to include mobile geo-location information, among other things.

Question 8. How does the Commission enforce whether operators have "actual knowledge" that their sites are used by children under 13? Is this scienter requirement an issue that merits additional scrutiny in your opinion?

Answer. As explained in the Statement of Basis and Purpose accompanying the COPPA Rule, actual knowledge will be present where the operator obtains direct information about a child's age or grade, for example, from a child's registration at a website or from a concerned parent who has learned that the child is participating at the site. In addition, the FTC has explained that it will examine closely websites that do not directly ask age or grade, but instead ask "age identifying" questions, such as "what type of school do you go to: (a) elementary; (b) middle); (c) high school; (d) college" and that through such questions, operators may acquire actual knowledge that they are dealing with a child under age 13.

The FTC has stated that the COPPA statute's actual knowledge standard does not require operators of general audience sites to investigate the ages of their website's

visitors or to monitor their chat rooms. However, an operator may be considered to have actual knowledge with respect to a specific child if someone from the operator's organization views a revealing post, or if someone alerts the operator to such a post (*e.g.,* a concerned parent who learns that his child is participating on the site).

Thus far, all of the FTC's COPPA cases involving "actual knowledge" center on an operator's direct receipt of information about a child's age input during the registration process.

The FTC staff has dedicated a panel at its June 2 COPPA roundtable to exploring the COPPA statute's actual knowledge standard.

Question 9. Are there any restrictions on state AGs enforcing compliance with the COPPA rule?

Answer. The COPPA statute permits state attorneys general to file civil actions on behalf of their residents in U.S. District Court to enjoin an operator's practices, enforce compliance with the FTC's COPPA Rule, obtain damages, restitution, or other compensation on behalf of their residents, or to obtain such other relief as the court deems appropriate. The statute places several minor limitations on a state attorney general's right to enforce COPPA. First, unless it would be infeasible to do so, an attorney general intending to enforce COPPA must provide the FTC with written notice and a copy of the complaint prior to filing the state action. Upon receipt of notice of a state's intent to enforce COPPA, the FTC has the right to intervene, to be heard, and to file a petition for appeal in the action. The statute also provides that any person or organization that has been approved by the FTC as a COPPA safe harbor program and whose guidelines are relied upon by a defendant as a defense may file as amicus curiae in a state COPPA proceeding.

To date, only one state—Texas—has provided notice to the FTC of its intention to enforce COPPA. In December 2007, Texas filed two COPPA actions, one against The Doll Palace Corp., and the other against Future US, Inc. (a/k/a *gamesradar.com*). Information about the Texas actions can be found at *http://www.oag.state.tx.us/oagNews/release.php?id=2288.*

Question 10. How is the *Net Cetera* distribution and education campaign working? Have the materials and the FTC's efforts to reach out to teachers and parents been effective?

Answer. The FTC issued a report to Congress about the *Net Cetera* campaign in March 2010, available at *http://www.ftc.gov/os/2010/03/100331netcetera-rpt.pdf.* This report discusses the creation of *Net Cetera*, how the FTC is getting the word out about the guide, and distribution highlights.

The *Net Cetera* education campaign continues to be a success. Since October 2009, the FTC has received orders for the Net Cetera guide from every state in the nation, for a total of over 3 million copies ordered in English and Spanish. Other outreach highlights include:

- Prince George's County Public Schools—the 2nd largest school district in Maryland and 18th largest in the Nation—distributed approximately 150,000 copies of *Net Cetera*.
- Public and school libraries across Massachusetts have received copies of the guide and are now placing orders, and every member of the Young Adult Library Services Association (YALSA) has received a copy.
- The National Association of School Nurses will distribute the guide to attendees at their upcoming annual conference.
- FTC staff are attending and speaking at conferences this summer to promote *Net Cetera*, including the widely-attended International Society for Technology in Education Annual Conference and the National School Public Relations Association National Seminar.
- Schools, police departments, and organizations in Arkansas have ordered over 34,000 copies of the guide.

Question 11. You mention 14 cases brought by the Commission over the past 10 years alleging COPPA violations. From your perspective, have those cases served to deter repeat violations or additional COPPA violations?

Answer. The FTC has been strategic in bringing cases that illustrate different core requirements. We have garnered widespread interest and significant leverage from each COPPA enforcement action addressing a particular type of violation. The FTC's early COPPA enforcement actions focused on children's sites that collected extensive amounts of personal information without providing notice to parents and obtaining their consent. Most recently, the FTC has focused on operators of both general audience and child-directed social networking sites and sites with interactive features that permit children to publicly divulge their personal information online.

Although law enforcement is a critical part of the Commission's COPPA program, the FTC's COPPA program is comprised of several effective integrated components—rulemaking, self-regulation, routine outreach to businesses and consumers, and law enforcement—that work in tandem to enhance overall COPPA compliance. The FTC believes that this integrated approach has served to deter repeat or additional violations.

Question 12. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

Answer. The COPPA statute applies to operators of commercial "websites located on the Internet" and "online services" that collect, maintain or disclose children's personal information on the Internet. Where children connect to websites or online services through mobile devices, the statute clearly applies. Where children are not connecting to or through websites or online services, COPPA may not apply. Thus, many, but not all, mobile communications may be covered by the statute. The FTC's Rule review will examine how the definitions of Internet, websites, and online services may affect COPPA's application to different mobile and other technological uses.

Question 13. [Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?]

Answer. N/A

Question 14. How do you propose to improve parental supervision and control of children's online activity to prevent the inappropriate or illegal collection and use of their information?

Answer. The FTC will continue to focus on educating parents, through tools such as *Net Cetera* and the agency's online safety portal, *OnGuardOnline.gov,* about the rights and protections provided by COPPA, and about children's online privacy and safety more generally.

Question 15. If you support a regime granting rules of the road for adolescents' privacy, how do you envision this sort of regime working? How would you propose it be structured? If you do not support a regime governing adolescents' privacy, please explain your reasoning.

Answer. The FTC's current review is focused on the COPPA Rule, and on the online privacy of individuals defined as children under that statute. The FTC has not yet had the opportunity to formulate an opinion on a possible regime to protect adolescents' privacy. The agency looks forward, however, to reviewing any proposals that may be put forward. In addition, last year, the agency released a set of principles relating to online behavioral advertising. Moreover, the Commission currently is examining privacy more broadly and hopes to develop a general privacy framework in the coming months.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO TIMOTHY SPARAPANI

Question 1. What steps is Facebook taking to promote the advancement of children's privacy?

Answer. Facebook provides users with innovative privacy controls to give users control of their information online. We have recently provided users with additional steps for controlling sharing both on Facebook and with third parties such as other websites or applications.

Facebook takes additional steps specifically targeted to minors. For example, we provide specialized privacy settings so that minors may further control their sharing through Facebook. In part, this eliminates the potential of minors sharing with everyone. Even minors who want to share with the maximum number of people may only share with users under 18 years of age. Additionally, Facebook provides special educational materials for minors. Furthermore, Facebook imposes rules requiring Facebook Pages and applications built by third parties on Facebook to impose age "gates" that work to prevent minors from accessing content that is inappropriate for their age or to be accessed through these Pages or Applications by non-minors.

Question 2. Do you think the age limit in COPPA is appropriate? And if so, why?

Answer. Facebook takes no position on the age limitations imposed by COPPA. We are not experts on the appropriate age to set for online activity, but our experience informs us that teenagers 13 years of age generally act in a responsible manner on Facebook.

Question 3. Do you think COPPA should be strengthened?

Answer. COPPA could be strengthened by providing incentives for companies to innovate without fear of liability to develop new technologies. The current legislative

and regulatory structure should encourage, not discourage continuing technological innovation.

Question 4. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

Answer. At this time, Facebook is not recommending an amendment to the definition of "personal information."

Question 5. In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

Answer. The U.S. Congress has failed to appropriate sufficient funds to ensure that the KIDS Act of 2008 actually is fully implemented. In particular, the KIDS Act requires the creation of a Federal list of Registered Sex Offenders (RSOs) but that list has not been completed. Because of this, Facebook prepares its own list—at Facebook's own expense—to help us periodically review our list of users and terminate accounts that might have been established by RSOs. Smaller companies, particularly application developers, do not have such resources and are unlikely to expend scarce resources to obtain a list of RSOs from all 50 states. Congress should encourage the Federal Government to build and maintain an up-to-date list of RSOs and distribute it to any company that asks for the list.

Furthermore, the U.S. Government should negotiate with foreign governments to obtain lists of those countries' RSOs to further support responsible companies' attempts to prevent access by RSOs to online services where minors may be present.

Question 6. What do you think is the most urgent update to COPPA needed?

Answer. Congress should explicitly create a safe harbor expressly permitting companies to explore technological and policy innovations to further limit the access of minors to sites that are inappropriate for their age, and to do so without fear of regulatory or legislative sanction. The current model discourages innovations that could advance the privacy, safety, and security of minors.

Question 7. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

Answer. Facebook does not categorize data as sensitive. Rather, all information is treated as sensitive and subject to disclosure subject to a user's privacy settings and only at the user's direction. Because we recognize that minors are special, we explicitly prohibit minors from sharing with groups of individuals wider than the classification of Friends of Friends and Networks, where minors' Networks are typically their classmates at their schools.

Question 8. Recent press reports have indicated that Facebook is making available to the Web user information that has been previously contained within closed networks. Which pieces of user information are or will be made publicly available without the user proactively making any changes to her privacy policy?

Answer. Contrary to press reports, Facebook does not make available to third parties information that was previously contained within closed networks. In December of 2009, Facebook eliminated Regional Networks that were established when Facebook's user base was much smaller. These Regional Networks provided any members of a particular network the opportunity to view content of any other participants. By eliminating these Regional Networks, Facebook enhanced minors' privacy substantially.

Further, in part to respond to this misinformation contained in press reports, Facebook recently provided our users with a single "global opt out" option to eliminate even any voluntary sharing with third parties.

Question 9. How does Facebook verify or authenticate its users' identities or ages?

Answer. As explained at length in our written and oral testimony, no company can actually "verify" any users' age. Instead, Facebook uses a series of novel, proprietary technologies to draw assumptions about the likelihood that a user is of age. Moreover, our users are required to provide us with their ages at the moment they create an account.

Question 10. Is Facebook tied or affiliated in any way with location-based advertising? Is it possible for a 14-year-old Facebook user to be tracked by other companies, devices or data gatherers without her knowledge or consent?

Answer. Facebook provides ads targeted to users based on their hometown. We never provide this piece of information to advertisers. To our knowledge, it is not possible for other companies, devices or data gatherers to track Facebook users using the users' Facebook information wither any users knowledge or consent.

Question 11. Could you describe your company's efforts to educate parents and teachers about online safety?

Answer. Since our inception, Facebook has worked assiduously to educate parents and teachers about online safety. Just last week, we were awarded an award from Wired Kids that we received, in part, due to our ongoing efforts to educate our users. Our staff speaks at an extraordinary number of events per year that are intended to perform this function. Our Safety and Privacy pages provide full explanations of how our users may fully utilize our innovative privacy settings and has been recently revised to offer specific sections with content tailored to different audiences, including parents, educators and teens.

Question 12. How do you work with law enforcement to combat Internet crime?

Answer. Our Chief Security Officer and the team he supervises work closely with governments throughout the U.S. and around the world to comply with lawful requests for assistance. Recently, Facebook provided the key information that helped secure the two largest CAN–SPAM Act judgments in history, leading to a substantial reduction in the amount of spam messaging our users are subjected to. On the rare occasion that Facebook identifies illegal material being circulated through our site we prevent the disbursement of that information and then report the content and the user account attempting to distribute that material to the National Center on Missing and Exploited Children and appropriate law enforcement. We would be happy to brief the Subcommittee at length about other assistance provided, within the scope of the law, to law enforcement.

Question 13. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

Answer. In addition to fully implementing the KIDS Act, the FTC should negotiate with foreign governments to encourage the sharing of foreign governments' RSOs with the U.S. Government and U.S. companies.

Question 14. Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?

Answer. Facebook supports the second five-year review of COPPA.

Question 15. How do you propose to improve parental supervision and control of children's online activity to prevent the inappropriate or illegal collection and use of their information?

Answer. We recommend that parents insist on being made friends on Facebook of their children, or, alternatively, that another adult friend or family member be made a friend of teenage users. Further, as mentioned previously, we have recently created additional educational materials targeted to parents to help them become more conversant with Facebook and tools to help safeguard minors' information.

Question 16. If you support a regime granting rules of the road for adolescents' privacy, how do you envision this sort of regime working? How would you propose it be structured? If you do not support a regime governing adolescents' privacy, please explain your reasoning.

Answer. Facebook prohibits users less than 13 years of age from using our service. We limit minors' sharing to reduce the scope of that sharing. Further, we give our users privacy controls to control virtually all of their information online. Any modification to COPPA or the regulations implementing it should recognize effective regimes such as that created by Facebook.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO MICHAEL D. HINTZE

Question 1. What percentage of your parental users take advantage of the parental controls offered by your software and services?

Answer. Although we know for the sites and services where we ask for age whether a user is under 13, we are unable to determine how many of our total users are parents. While reliable data specific to Microsoft's products and services is not available, research by the Henry J. Kaiser Family Foundation found that 41 percent of parents report using parental controls to block their children's access to some websites.[1]

Question 2. You said in your written statement that "Microsoft proactively requests age information and seeks parental consent for children's use of many of its services even when those services are not specifically targeted to children." What formula do you use to determine whether to seek parental consent for children's use of services that are not specifically targeted to children? (How do you make that determination and could you give the Committee some examples of those services?)

---

[1] Henry J. Kaiser Family Foundation, Parents, Children & Media, at 11 (June 2007), *http://www.kff.org/entmedia/upload/7638.pdf.*

Answer. Our approach goes beyond COPPA in that we screen for age and obtain parental consent for under–13 users not only on our sites and services that are "targeted" to children, but also on our general audience sites that are "attractive" to children.[2] We do not have an exact formula for determining which sites or services may be attractive to children, but some examples of general audience services where we have decided to screen for age and seek parental consent for users under 13 include Hotmail, Messenger, Windows Live Spaces and Xbox Live.

Question 3. Do you think the age limit in COPPA is appropriate? And if so, why?

Answer. Yes, we believe the age limit in COPPA is appropriate. It is certainly true that COPPA's stated goals of increasing parental involvement and protecting privacy are important with respect to teenagers. But COPPA's existing structure and parental consent processes are not well suited to deal with this age group. For example, teens are too sophisticated to be deterred by age gates, and existing parental consent mechanisms—such as the toll-free number and print and send methods—may not be reliable in ensuring it is the parent rather than the teen who is giving consent.

In addition, teens' use of the Internet raises somewhat different privacy and safety issues than for children under thirteen. For example, while older teens may be more likely to understand the implications of online advertising than young children, teenagers may be more likely to be faced with instances of cyberbullying online.[3]

We believe there are alternative ways to protect the privacy of teens online that are better than simply expanding COPPA's age limit. For instance, Microsoft provides parents with a number of educational resources and technology tools so that they can talk to their teens about the importance of privacy and safety online and be more involved in their online activities. Additionally, Microsoft has long supported comprehensive Federal privacy legislation that would establish baseline protections and enhance the privacy of all individuals—including teens.[4] We are committed to working with Congress to advance these important efforts.

Question 4. Do you think COPPA should be strengthened?

Answer. We do not believe that amending the statute is necessary at this time. The statute provides the FTC with sufficient authority and flexibility to address children's privacy issues in light of evolving technologies and business models. We commend the Commission for launching its review of the COPPA Rule, which had been planned for 2015, 5 years early in order to account for new technologies. At the very least, we believe it would be prudent to allow the FTC to complete its Rule review before determining whether legislative action is necessary.

Question 5. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

Answer. Yes, the FTC should reexamine the definition of "personal information," and we are pleased that they have indicated an intent to do so. With its flexible definition of personal information, the COPPA statute is sufficiently forward-looking and gives the FTC the rulemaking authority to address evolving circumstances and needs. Therefore, we believe that the FTC, within the parameters of the existing statute, can update the definition of "personal information" included in the COPPA Rule to address the wide range of factors that have changed over the last decade.

Question 6. In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

Answer. Criminals who prey on children and families are the biggest threat to children's privacy and safety. To help thwart these criminals, Microsoft works with lawmakers in many countries to promote stronger online safety and privacy legislation and Internet safety education in schools. We help train law enforcement personnel in using technology to help combat online child pornography, child predators, and child exploitation. We use a filtering tool to review images uploaded to Windows Live Spaces and other Microsoft online properties to detect potential instances of child exploitation. And we are working with law enforcement officials in several

---

[2] *See* Microsoft Corp., *Privacy Guidelines for Developing Software Products and Services*, Section 1.11 and Scenario 8, available at *http://download.microsoft.com/download/0/8/2/082448D8-2AED-45BC-A9A0-094840E9E3A2/Microsoft_and%20Privacy_guidelines_for_developers.doc*.

[3] *See* Amanda Lenhart, Pew Internet & American Life Project, "Cyberbullying 2010: What the Research Tells Us" (May 6, 2010), *http://www.pewinternet.org/~/media//Files/Presentations/NCMEC_Cyberbullying%20talk%20050610release.ppt*.

[4] *See, e.g., http://www.microsoft.com/presspass/features/2005/nov05/11-03Privacy.mspx*.

countries to deploy the Child Exploitation Tracking System ("CETS"), a software tool to help investigators share and analyze information for tracking child exploitation on the Internet. We are committed to working with Congress, Federal and state agencies, nonprofit organizations, and other industry leaders to help protect children's privacy and safety in today's online world.

Question 7. What do you think is the most urgent update to COPPA needed?

Answer. We do not believe that the COPPA statute needs to be updated at this time. As explained in my testimony, we believe that the best course is for the FTC to update the COPPA Rule by providing clear guidance on how companies can better meet both the letter and the spirit of the law in light of changing technologies and by addressing the weaknesses of the currently approved approaches to obtaining verifiable parental consent.

Question 8. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

Answer. Under COPPA, any personal information collected from children under the age of 13 triggers the obligations of the Act, including the requirements for verifiable parental consent. We believe this broad approach is appropriate given the unique sensitivities involved with the collection and disclosure of data from young children.

Question 9. How does Microsoft handle location information? And what is the company's relationship with location tracking applications?

Answer. Microsoft is a leader in developing privacy standards to protect users of location-based services. In 2004, Microsoft partnered with TRUSTe and AT&T Wireless to form the Wireless Advisory Committee, which works with companies providing wireless data and wireless web services to ensure that specific standards regarding consumer notice and consumer consent are achieved.[5]

We expect to offer some location-based services on our platforms in the upcoming months. These location-based services may include local search, camera, mapping, and phone finder applications and services that utilize a user's current location.

Microsoft is committed to providing users control over their location-based data. On our platforms, users must first agree to allow Microsoft to access or use their current location, and users can always disable the sending of location information if they change their minds. Microsoft does not currently offer any services that disclose a user's location to others or that allow users to be tracked by third parties.

Question 10. You mention a "digital identity card" as one technology that could enhance authentication and streamline parental consent processes? Could you elaborate upon your idea?

Answer. Over time robust digital identity cards may become analogous to tangible cards in a person's wallet. In much the same way that a person might use a student ID card to get free admission to a museum, one or more digital identity cards may be used to verify the card owner's identity or an identity attribute, such as age or parental status.

To accomplish these types of verification, one way that digital identity cards could be issued is through offline processes where approved verification of a parent-child relationship already occurs. Website operators and online service providers could verify age and obtain parental consent by requesting that parents and children provide their digital identity cards before a child may access interactive services and features. These types of technologies still require that robust proofing and authentication processes occur, but can facilitate the online use and reuse of the proofing. Like with other solutions, they are not foolproof and should be used in conjunction with education and other online safety tools, including technologies that help balance against the disclosure of information that is not needed to verify the identity of the child or the parent.

Question 11. Does Microsoft have any other ideas for new parental control methods that would not cause additional privacy concerns or be tied to an IP address?

Answer. Microsoft recommends that the FTC expand its list of approved parental consent methods to include other reliable approaches that minimize burdens on parents, leverage existing technologies, and scale for millions of users. Because children are increasingly using mobile phones and other mobile devices, we also urge the FTC to consider the types of parental consent mechanisms that are appropriate for online services that are accessed through these devices.

---

[5] TRUSTe, "TRUSTe Announces First Wireless Privacy Standards to Protect Mobile Users" (Feb. 18, 2004), *http://www.truste.com/about_TRUSTe/press-room/news_truste_announces_first_wireless_privacy_standards.html.*

Microsoft is working on technology that enables parents and children to better manage their identities online in a privacy enhancing way. When combined with the use of digital identity cards, these technologies could allow parents and children to disclose only that information that is necessary (such as parental status or age, but not name or other personal information) to enable children's access to and use of websites and online services.

Question 12. In your "Family Safety at Microsoft" attachment submitted to the Committee, you state, "In the United States, 71 percent of teens with online access have a social networking profile." What are the implications of this statistic for our discussion? Are children using common sense when using the Internet? Do trends indicate that young children are disclosing information they shouldn't and what are companies doing with that information?

Answer. Given the percentage of teens that are using social networks, it is important that teens with online access be taught how to use such services wisely and safely. To this end, Microsoft is a member of the Ad Council's Internet Safety Coalition, which is working to help kids understand that the Internet is a public place and to explain the risks of ill-considered Internet posting. Microsoft also provides parents with a number of educational resources and technology tools so that they can talk to their teens about the importance of privacy and safety online and be more involved in their online activities.[6] We are committed to working with Congress to make sure parents, educators, and children are aware of these resources and take advantage of them. Microsoft has no special insight into the types of information that children are disclosing online in general or into the privacy practices of other companies.

Question 13. Could you describe your company's efforts to educate parents and teachers about online safety?

Answer. While Microsoft has created a number of tools and technologies to help promote child privacy and safety on the Internet, we believe that educating parents, teachers, and children is one of the most effective ways to respond to online risks. To this end, we offer a number of educational resources for parents, teachers, and children regarding the importance of online privacy and safety.[7] We also support numerous family safety educational organizations and outreach efforts. For example, Microsoft is a sponsor of i-SAFE America's i-LEARN program, which provides free online curriculum for educators, parents, and teens.[8] We helped to create, along with other technology companies, the National CyberSecurity Alliance, whose mission is to educate all users, including parents and children, about how to stay safe online.[9] Microsoft also supports GetNetWise, a public education organization that offers Internet users resources for making informed decisions about safer Internet use.[10] A representative list of Microsoft's educational efforts is provided in the attachment to my written testimony.[11]

Question 14. How do you work with law enforcement to combat Internet crime?

Answer. Microsoft is committed to helping make the Internet safer for all users—including children and families—but we can't do it alone. Therefore, Microsoft partners with law enforcement agencies to combat Internet crime.[12] For example, Microsoft has partnered with the National Center for Missing and Exploited Children ("NCMEC") to develop and deploy technology solutions that disrupt the ability of online predators to exploit children or traffic in child pornography. We also have worked with Interpol and the International Centre for Missing and Exploited Children ("ICMEC") to sponsor worldwide training sessions for law enforcement personnel on computer-facilitated crimes against children. In addition, Microsoft works extensively with the Department of Justice's Internet Crimes Against Children Task Force and has worked with a number of state Attorneys General to provide comprehensive training for law enforcement on computer-facilitated crimes.

Question 15. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

Answer. One of the advantages of the COPPA statute is that it provides a flexible framework by which the FTC can quickly adapt its rules to accommodate advanced technologies, including mobile devices. The FTC recently launched a proceeding to

---

[6] *See http://www.microsoft.com/protect/family.*
[7] *See http://www.microsoft.com/protect/family.*
[8] *See http://www.ilearn.isafe.org.*
[9] *See http://www.staysafeonline.org/.*
[10] *See http://www.getnetwise.org.*
[11] See pp. 7–8, available at *http://download.microsoft.com/documents/uk/education/homeaccessprogramme/FamilySafety-US.pdf.*
[12] *See id.* at 9–10.

look into this issue, and Microsoft will be participating in that process. We believe that the FTC can strengthen children's safety and privacy online by providing clear guidance on how companies can better meet not only the letter, but also the spirit, of the law in light of advanced technologies and by addressing the weaknesses of the currently approved approaches to obtaining verifiable parental consent. We do not believe that amending the statute is necessary at this time. At the very least, we believe it would be prudent to allow the FTC to complete its Rule review before determining whether legislative action is necessary.

Question 16. Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?

Answer. Yes, we agree with the direction the FTC is taking for its COPPA Rule review. We commend the FTC for taking the initiative to launch its review 5 years early in light of children's increasing use of new technologies to access the Internet. We expect that the FTC's comprehensive review process will produce a strong public record that will help inform the FTC as it considers whether modifications of the COPPA Rule are needed.

Question 17. How do you propose to improve parental supervision and control of children's online activity to prevent the inappropriate or illegal collection and use of their information?

Answer. We recommend that the FTC update two key aspects of the COPPA Rule in order to improve parental supervision and control of children's online activity. First, we hope that the FTC will use its review process to encourage companies that provide sites and services that are attractive to children to be more proactive about creating opportunities for parental engagement in their children's online activities. Second, we urge the FTC to work with technology companies and consumer advocates to develop more consumer-friendly, effective, and scalable methods for obtaining parental consent, especially in the context of mobile devices.

We also believe in empowering parents through parental controls. To this end, we make available tools for a number of our services, such as Windows Live and Xbox Live, that help parents make granular choices about how their children may share personal information online. For example, Microsoft's parental controls enable parents to limit their children's searches, block (or allow) websites based on the type of content, restrict with whom their children can communicate, and access detailed activity reports that show the websites their children visited and the games and applications they used.

Question 18. If you support a regime granting rules of the road for adolescents' privacy, how do you envision this sort of regime working? How would you propose it be structured? If you do not support a regime governing adolescents' privacy, please explain your reasoning.

Answer. Microsoft has long supported comprehensive Federal privacy legislation that would establish baseline protections and enhance the privacy of all individuals—including adolescents.[13] In addition, we believe that a key element of protecting privacy for adolescents is to find ways to effectively encourage parental involvement in their online activity. Microsoft provides parents with a number of educational resources and technology tools so that they can talk to their teens about the importance of privacy and safety online and be more involved in their online activities. We are committed to working with Congress to advance these important efforts.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO KATHRYN C. MONTGOMERY

Question 1. Do you think the age limit in COPPA is appropriate? And if so, why?

Answer. The regulations that were put in place for COPPA are appropriate for children under the age of 13, and were designed to provide protections specifically for this age group. They are part of a long tradition of advertising policy safeguards that are based on social science research dating back to the 1970s. However, because COPPA only covers young children, online marketers have developed a spectrum of techniques for data collection and targeting focused on adolescents, with virtually no government oversight. Recent research in neuroscience and adolescent development has identified a number of ways in which adolescents are vulnerable to new forms of marketing, particularly in the digital context (See articles by Professors Frances Leslie and Constance Pechmann at the University of California, Irvine at *digitalads.org.* See also Kathryn C. Montgomery and Jeff Chester, "Interactive

[13] *See, e.g., http://www.microsoft.com/presspass/features/2005/nov05/11-03Privacy.mspx.*

Food and Beverage Marketing: Targeting Adolescents in the Digital Age," Special supplement to *Journal of Adolescent Health*. September, 2009: 1–12.) New legislation is needed to provide adolescents with substantive protections from unfair data collection and marketing practices.

Question 2. Do you think COPPA should be strengthened?

Answer. Under its current review of COPPA, the FTC needs to ensure that the rules are updated to apply to evolving data collection and targeting practices. These include: behavioral profiling, ad networks, social networking platforms, location targeting and other mobile practices, etc. COPPA legislation was drafted with sufficient flexibility to accommodate these new practices, but they need to be articulated clearly in the updated FTC rules to ensure that the law is implemented effectively.

Question 3. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

Answer. The FTC should reexamine the definition of Personal Information in COPPA. Its current definition only covers a few examples of what constitutes personally identifiable information. However, the law includes a clause (SEC. 1302 8, F) that was designed to ensure that evolving practices are included in the definition of personal information: "any other identifier that the Commission determines permits the physical or online contacting of a specific individual." With the growth in behavioral profiling practices, digital marketers can now use a variety of new identifiers, including IP address, cookies, and other "passive" forms of data collection, to easily identify and target an individual child. As the work of Professor Paul Ohm at the University of Colorado shows, the ability of data bases to re-identify individuals is growing. Narrow definitions of PII do not capture how industry treats data about individuals.

The FTC has already recognized the need to expand the definition of personally identifiable information in some of its other documents, including the FTC Staff Report on Self Regulatory Principles for Online Behavioral Profiling (Feb, 2009), which recognizes that Personal Information can include the tracking of given devices, computers or browsers. The European Commission's Article 29 Working Party has also articulated the need to redefine personal information.

Question 4. In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

Answer. The biggest threat is the creation of a vast infrastructure for data collection in a variety of networked technologies and platforms used by children and adolescents. Current and emerging industry practices are designed to maximize data collection while minimizing transparency. Each new technology available to the public brings with it a new way for data collection to occur, and little if any discussion about the impact or planned uses of this data.

Question 5. What do you think is the most urgent update to COPPA needed?

Answer. As outlined above, the most urgent need is to ensure that current regulatory and self-regulatory safeguards are applied to new platforms and practices for data collection and targeted marketing.

Question 6. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

Answer. Any data about children and teens should be considered sensitive. In many ways, both children and adolescents are "sensitive users," who should be afforded special protections. Teens and children have limited developmental capacities for understanding fully the trade-offs involved in today's data collection and marketing environment.

Question 7. Do you think any incentives exist for children to refrain from revealing information about themselves or do you think there is momentum encouraging young people to surrender their privacy?

Answer. Revealing information is necessary for even the most basic of social and developmental interactions online. The most insidious data collection that occurs is the through surveillance by marketers of interactions that teens have with their friends, family, schools etc. (particularly on social networks). Policy should focus on protecting data, involving parents, and regulating data collectors, rather than discouraging children from interacting.

Question 8. You helped negotiate COPPA when it was created and so you are familiar with its bipartisan nature and flexibility. Do you believe the statute is sufficiently responsive to the challenges facing young people as much of their information appears to be mined and collected?

Answer. Those of us who negotiated COPPA understood that we were dealing with a new system of online marketing and data collection that would be undergoing dramatic growth and change during the ensuing years. One of the law's purposes, from my vantage point, was to ensure that a system of safeguards was put in place during the earliest stage of ecommerce in order to guide the development of future practices and to establish a clear set of principles that young people needed protections from unfair marketing and data collection. The language in the original statute provides a mechanism for ongoing review by the FTC to ensure that these safeguards are adapted to take into account the evolving practices and platforms of the growing digital media and marketing environment. However, these FTC reviews must be thorough, accurate, and timely enough to ensure that this original intent is carried out.

Question 9. Researchers have suggested that marketers today can identify in real time where kids are, who their friends are, and what they are doing—representing some real privacy issues. Could you elaborate upon how this tracking works and what it could mean for young people's security and privacy?

Answer. Advances in what is called "computational advertising" now permit real-time tracking and targeting of online consumers (including youth) across a variety of platforms, employing a range of data collection and analysis techniques through cookies, tracking pixels, location and social networking data. "Social media marketing" applications, for example, can tap into social networks to identify a particular individual and his or her networks of friends (through what is called the "social graph.") Sophisticated data mining tools enable stealth analysis of the content and communications people post to their social networking profiles, including videos, photos, music, etc. These practices not only subject young people to increasing numbers of third party marketers, but also make them vulnerable to others who may be able to learn their location, interests and relationships. Social media marketing is growing very rapidly, raising a number of serious questions about the need for additional safeguards to protect children and adolescents.

Question 10. Your testimony includes the following remark: "Ads on mobile phones will be able to reach young consumers when they are near a particular business and offer electronic pitches and discount coupons." Does this mean that a 13-year old with a mobile device could receive undesired targeted ads based on her geographic location and proximity to a specific business? Do you believe that is problematic?

Answer. Location targeting permits tracking and targeting of consumers (including youth) via their mobile devices. Increasingly as individuals' locations are made available to third parties, mobile users will be marketed to in "real-time" via mobile coupons and other offers based on where they may be at a particular time (or based on analysis of their moves from and to various locations over time). Federal policies are needed to regulate mobile marketing to both children adolescents, and to ensure that real-time location and other behavioral information is kept private. Rules are also required to ensure meaningful opt-in policies that clearly and prominently explain how the data are collected and used, as well as limits on the duration of location targeting consent.

Question 11. The extent to which children understand how their information is being used is worth discussing. You state in your testimony, "When COPPA was created, one of our concerns was to ensure that the ability to identify, track, and target a child—whether online or off—was mediated through Congressional safeguards mandating parent involvement. And while young people—and adults—today are being continually urged to make more of their personal information available in real-time, including their location, research indicates [that] few people understand how that information is being collected and used." How is young people's information being used and to what extent are they aware of its use and collection?

Answer. Research at UC Berkeley and the Annenberg School for Communication at the University of Pennsylvania has documented that the majority of the public, including youth, care very much about protecting their privacy in the online environment. However, all online consumers confront a non-transparent, pervasive, and largely unaccountable data collection system. Many youth oriented commercial sites encourage youth to give up large amounts of information about themselves and their friends without fully explaining how that information will be used. A growing number of specialized data mining and behavioral targeting companies are tracking the behaviors of individuals as they conduct their daily activities on the Internet, including searching for health or other information, and interacting with friends on social networks, with very little disclosure of how the marketing apparatus functions.

Question 12. You wrote in your written statement: "Social networks have created privacy settings that create a false sense of security for teens." What did you mean by that remark?

Answer. Social network privacy settings often are aimed at limiting how data is shared or made available to other social network users. They do not address how the social network, its advertisers, or third party applications retain and use the data. Nor may the settings be that effective, allowing someone who may be a casual acquaintance, but listed as a "friend," gain access to your information. Companies such as Facebook and MySpace may enable users to restrict who has access to their profiles and activities, but these companies do not adequately inform users about the nature and extent of commercial practices on these networks, involving data collection, surveillance, and behavioral profiling.

Question 13. You advocated for a regime to protect adolescents' privacy. How do you envision this sort of regime working? How would you propose it be structured?

Answer. Adolescents should receive protections in line with the Fair Information Practices principles created by the OECD, as well as a set of more granular safeguards developed specifically for this age group. (See below for additional information in response to this question.)

Question 14. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

Answer. The recent oversight hearing by the subcommittee chaired by Sen. Pryor (along with the participation of Commerce Committee Chairman, Sen. Rockefeller) has already helped underscore why ensuring protecting the privacy of young people is a key public policy concern. I urge the Committee to oversee the work of the FTC in this area, and to conduct additional hearings, including a review of the final recommendations made by the FTC on new COPPA implementation rules. I also urge the Subcommittee to conduct hearings and introduce new legislation designed to protect adolescent privacy online.

Question 15. Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?

Answer. Through its 2010 evaluation of COPPA, the FTC is working to address how the implementation of the law can better protect children under 13. I believe the FTC should also conduct independent research to document how young people's data is being collected from new practices, including behavioral targeting and mobile marketing. Because so many of these practices are not transparent, the Commission should be encouraged and, if need be, specifically authorized, to conduct investigations of contemporary advertising and data collection in the children's digital marketplace, and should use its subpoena power to solicit data from industry about how it interacts with children.

Question 16. How do you propose to improve parental supervision and control of children's online activity to prevent the inappropriate or illegal collection and use of their information?

Answer. The FTC should include in its current review an analysis of how well parents are able to rely on the current parental verification mechanisms and whether any of these mechanism have created loopholes that enable marketers to target individual children inappropriately. This should include reviewing currently approved safe harbor regimes to determine whether outside parties may have access to young people's data.

Question 17. If you support a regime granting rules of the road for adolescents' privacy, how do you envision this sort of regime working? How would you propose it be structured? If you do not support a regime governing adolescents' privacy, please explain your reasoning.

Answer. I would support broad legislation to protect all consumers, based on a framework of fair information principles. Within that framework, additional safeguards should be established to address specifically the needs of youth age 13–17, who are not covered by COPPA. A Fair Marketing Digital Bill of Rights for Teens would balance the ability of young people to participate fully in the digital media culture—as producers, consumers, and citizens—with the governmental and industry obligation to ensure adolescents are not subjected to unfair and deceptive surveillance, data collection, and behavioral profiling by marketers. The onus of responsibility should not only be placed on youth to protect themselves, but also on the companies that market to them. Fair marketing and data collection rules are needed to help ensure that young people are socialized to be responsible consumers in the growing digital marketplace, and to understand their rights to privacy.

While some elements of COPPA could serve as a useful model for adolescent online privacy policy, I do not believe the mechanism for parental approval is appropriate or advisable in the case of teens. The legislation should include:

- The principle of maximizing user control over their information while minimizing data collection.
- Congressional authorization that directs the FTC to conduct research, hold workshops, and develop rules to ensure consumer protections for teens in digital marketing, with a special focus on data collection and behavioral profiling.
- Effective, full disclosure of marketing and data collection practices with meaningful opt-in:
  - User-friendly, granular information that is prominently displayed at times and in places where teens will read and understand it.
  - Opt-in mechanisms that are tailored to a variety of digital platforms, including mobile, social networks, etc.
- Limitations on the amount of data, types of data, and retention of data collected from adolescents for digital marketing purposes.
- Limitations on behavioral profiling and targeting of adolescents, as well as restrictions on other practices that may take advantage of under age youth, such as sharing with third parties, retargeting, location targeting, and computational advertising.
- Special privacy rules for social networks, mobile, and interactive games.
- Like COPPA, a government regulatory framework, along with self-regulatory regimes that create a level playing field for both consumers and businesses by implementing "rules of the road" for marketing to teens.
- Mechanisms for accountability and independent assessment, and fines for failure to comply with rules.
- Built in flexibility of rules to ensure continued effectiveness as digital marketing practices evolve and expand.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO BERIN SZOKA

Thank you, Chairman Pryor, for the opportunity to supplement my written testimony from this hearing by responding to your questions.[1] In my responses, I have incorporated some of the material found in the comprehensive survey of the perils of expanding COPPA's scope beyond its original, limited purposes (what we have called "COPPA 2.0") that my colleague Adam Thierer and I published in May 2009: *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*.[2] Further detail on many of the points below can be found in that paper.

I. A Reexamination of COPPA

It bears repeating at the outset that the Federal Trade Commission's (FTC) current proceeding is not examining the Children's Online Privacy Protection Act ("COPPA") itself (the statute),[3] but rather the "COPPA Rule" (the regulations mandated by the agency pursuant to COPPA).[4] The agency is well aware of this distinction—and, indeed, far more precise about it than probably any interested party. For example, the agency's recent inquiry is titled "Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule."[5] But it is a distinction that is far too often lost on many advocates who are lobbying for change.

Congress, of course, retains the authority to change the COPPA statue at any time, and it is well within the jurisdiction of this committee to consider doing so. But in re-examining COPPA, lawmakers should tread carefully. *Any attempts to reopen COPPA to expand the statute beyond its original, limited purposes could raise*

---

[1] Written Testimony of Berin Szoka, Hearing on "An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act" before the Subcommittee on Consumer Protection, Committee on Commerce, Science, and Transportation, U.S. Senate, April 29, 2010, *www.pff.org/issues-pubs/testimony/2010/2010-04-29-Szoka__Written__COPPA__Testimony.pdf*.

[2] Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech,* Progress on Point 16.11, May 2009, *http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-ageverification.pdf ("COPPA 2.0")*.

[3] 15 U.S.C. §§ 6501–6506.

[4] 16 C.F.R. Part 312.

[5] Federal Trade Commission, *Children's Online Privacy Protection Rule: Request For Public Comment on the Federal Trade Commission's Implementation of the Rule*, 75 Fed. Reg. 17,089, April 5, 2010, *http://www.ftc.gov/os/2010/03/100324coppa.pdf* (*COPPA Implementation Review*).

serious constitutional questions about the First Amendment rights of adults as well as older teens and site and service operators, and also have unintended consequences for the health of online content and services without necessarily significantly increasing the online privacy and safety of children.

A. Do you think the age limit in COPPA is appropriate? And if so, why?

Yes, and understanding why is the key to understanding the delicate balance of COPPA in general. The COPPA Rule's requirements are relatively easy for site and service operators to implement, and for the government to enforce, because they apply only to the collection of information about children under 13 by commercial operators (or the public sharing of information by children themselves) only when: (i) the operator's site or service is "directed to children" or (ii) the operator has actual knowledge that they are collecting personal information from a child. But the key practical difficulty in implementing a COPPA 2.0 system for adolescents 13 and above is in the anonymity inherent in the technical architecture of the Internet. To quote a memorable cartoon from *The New Yorker*: "On the Internet, nobody knows you're a dog."[6] Because website operators generally do not know who is accessing their site, requiring any special treatment of minors is tantamount to requiring age-verification of all users.[7] Again, COPPA's ingenious solution to this problem is that the law applies only to the limited "Internet Jr." of sites "directed at children," or in cases where an operator has "actual knowledge" that it is dealing with a child.

Because "child-oriented" websites are generally easy to define and are very rarely used by adults, COPPA's age verification mandate has not significantly impacted the free speech rights of adults because few adults other than parents ever want to use these sites, and parents essentially are already age verifying themselves in the process of providing "verifiable trial consent" for their children (those under 13). But it is *far* more difficult to define a class of "adolescent-oriented" websites (*i.e.,* "directed at" kids age 13–17, as proposed in New Jersey in 2008[8]) that are not also used by significant numbers of adults. The practical result of such COPPA expansion efforts would be the same as simply specifying that a certain category of websites (such as those with a public "wall," as proposed in Illinois in 2008[9]) must age-verify of a large number of adults to distinguish adults (who do not require verifiable parental consent) from children (who do require verifiable parental consent). This raises profound First Amendment concerns—particularly about the right of Americans to speak and receive information anonymously online.[10]

It was at least in part in recognition of the difficult First Amendment questions discussed below that Congress removed the requirement in the initial legislative draft of COPPA that would have required operators to "use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[11]

---

[6] Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, THE NEW YORKER, July 5, 1993, at 61, available at *www.unc.edu/depts/jomc/academics/dri/idog.html* (cartoon of a dog, sitting at a computer terminal, talking to another dog).

[7] Of course, the COPPA's second prong of age-verification requirement applies only when the website operator has "actual knowledge" that the user is a minor. 16 C.F.R. § 312.3.

[8] A.B. 108, Gen. Assem., 213th Leg. Sess. (N.J. 2008), *www.njleg.state.nj.us/2008/Bills/A0500/108_I1.HTM*.

[9] H.B. 1312, 96th Gen. Assem., Synopsis as Introduced (Il. 2007) [hereinafter *SNWARA*], available at *www.ilga.gov/legislation/billstatus.asp?DocNum=1312&GAID=10&GA=96&DocTypeID=HB&LegID=43038&SessionID=76.*

[10] *See infra* at 3–9.; *see generally, COPPA 2.0, supra* note 2; Adam Thierer, The Progress & Freedom Foundation, *USA Today, Age Verification, and the Death of Online Anonymity*, PFF Blog, Jan. 23, 2008, *http://blog.pff.org/archives/2008/01/usa_today_doesn.html*. 4

[11] This requirement was contained in the original bill, Children's Online Privacy Protection Act, S. 2326, 105th Cong. § 3(a)(2)(A)(iii), (1998), but was removed when that bill was reintroduced in its final form. In the interim, Congress held a hearing at which testimony was offered by, among others, Deirdre Mulligan, on behalf of the Center for Democracy and Technology, which generally supported COPPA but argued for the very revisions that were ultimately made. In particular, Mulligan argued that:

> under the bill each time a 15 year old signs-up to receive information through e-mail his or her parent would be notified. For example if a 15 year old visits a site, whether a bookstore or a women's health clinic where material is made available for sale and requests information about purchasing a particular book or merely inquires about books on a particular subject (abuse, religion) using their e-mail address the teenager's parent would be notified. This may chill older minors in pursuit of information.

Testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology, before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Communica-

Continued

These First Amendment concerns are not conjectural: The courts have already struck down precisely this kind of broad age verification mandates—specifically, as found in the Children's Online Protection Act (COPA),[12] another 1998 law sometimes confused with COPPA. In essence, COPPA is focused on certain kinds of potentially harmful *contacts* while COPA is focused on potentially harmful *content*.[13] COPA attempted to prevent children from accessing material deemed "harmful to minors" by requiring all users attempting to access such content to provide a credit card, on the theory that only adults have credit cards. But the courts concluded that, "payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards" and, although "payment card issuers usually will not issue credit and debit cards directly to minors without their parent's consent because of the financial risks associated with minors . . . there are many other ways in which a minor may obtain and use payment cards."[14]

1. COPPA's Current Age Range Respects the First Amendment Rights of Adults

Besides the fact that credit cards were simply inadequate for proving that someone was not a child (a very different problem from obtaining verifiable parental consent, as discussed below), the court held that requiring adults to prove that they were not children by providing credit card information violated the First Amendment in a number of ways.

First, COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial ."[15] In 2008, in striking down COPA for the third and final time, the Third Circuit approvingly quoted the district court, which had noted that part of the reason age verification requirements deterred users from accessing restricted content was "because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet."[16] The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication.[17] By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves *more* protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz.,* pornography), COPPA 2.0 would burden access to material by adults as well as minors, not because that material is harmful or obscene, but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications of a political nature, which deserve the highest degree of First Amendment protection.

Second, COPA burdened the speech rights of operators because the necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is reducing the audience of those sites. Similarly, if COPPA's age ceiling were raised to cover adolescents, some websites would self-censor themselves to avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate for all users—or to legal liability if they failed to implement

---

tions, Sept. 23, 1998, *http://web.archive.org/web/20080327000913/http://www.cdt.org/testimony/980923mulligan.shtml.*

[12] 47 U.S.C. § 231.

[13] COPA makes it illegal to "knowingly . . . make[ ] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. 231.

[14] *ACLU* v. *Gonzales*, 478 F. Supp. 2d 775, 801 (E.D. Pa. 2007) [hereinafter *Gonzales*]. COPA would have prohibited the online dissemination of material deemed harmful to minors under 17 for commercial purposes, 47 U.S.C. § 231(a)(1), subject to a safe harbor for sites that made a "good faith" effort to restrict access by minors: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology," 47 U.S.C. § 231(c)(1).

[15] *ACLU* v. *Ashcroft*, 322 F.3d 240, 259 (3d Cir. 2003) (*ACLU II*).

[16] *ACLU* v. *Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (ACLU III) (citing *Gonzales*, 478 F. Supp. 2d 775 at 806).

[17] *McIntyre* v. *Ohio Elections Comm'n,* 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also Talley* v. *California*, 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

age verification. The substantial cost of age verification could significantly impact, if not make impossible, the razor-thin business models of many sites, which generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[18]

Third, courts held that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[19] Similarly, parental control software already empowers parents to restrict their kids' access to websites and similar software is evolving for mobile services and smartphone software (*i.e.,* applications or "apps") that would offer parents control over what services kids use that allow them to share their personal information, either with operators or with other users.

Finally, it's worth noting that COPPA 2.0 would restrict the ability of adolescents to access content (in interactive contexts where they might also share personal information), not because it could be harmful to them or because it is obscene, but merely because it is "directed to" them. While the First Amendment rights of minors may not be on par with those of adults, adolescents *do* have the right to access certain types of information and express themselves in certain ways.[20] The Supreme Court has held that "constitutional rights do not mature and come into being magically only when one attains the state-defined age of majority."[21] It remains unclear how an expanded COPPA model might interfere with the First Amendment rights of adolescents, but it is clear that privacy and speech rights would come into conflict under COPPA 2.0, as they do in other contexts.[22]

For example, how might the parental-consent based model limit the ability of adolescents to obtain information about "safer sex" or how to deal with trauma, depression, family abuse, or addiction? Would an abusive father authorize a teen to visit a website about how to report child abuse? Would parents of adolescents struggling with their sexual identity let their children participate in a self-help social networking page for gay and lesbian youth?[23] The rights are at play here are critically important and must be balanced carefully.

---

[18] *See ACLU III*, 534 F.3d at 196–97 (citing *Gonzales*, 478 F. Supp. 2d 775 at 804). The Court held that websites "face significant costs to implement *COPA's age verification mandates+ and will suffer the loss of legitimate visitors once they do so." *Id.* at 197.

[19] *Id.* at 198 (quoting *ACLU* v. *Mukasey*, 534 F.3d 181, 198 (2008)).

[20] *See* Theresa Chmara & Daniel Mach, *Minors' Rights to Receive Information Under the First Amendment,* Memorandum from Jenner & Block to the Freedom To Read Foundation, Feb. 2, 2004, *www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/minorsrights.cfm* (summarizing case law regarding minors' first amendment rights, especially in schools and in the context of mandates that public libraries filter Internet content); *United States* v. *Am. Library Ass'n*, 123 S. Ct. 2297 (2003), available at *laws.findlaw.com/us/000/02–361.html* (upholding the constitutionality of a filtering software system applicable to minors); *see generally, Tinker* v. *Des Moines Ind. Comm. School Dist.*, 393 U.S. 503 (1969) (upholding students' rights to wear protest armbands and affirming that minors have speech rights), available at *www.oyez.org/cases/1960–1969/1968/1968_21*; cf. *Morse* v. *Frederick*, 551 U.S. 393 (2007), available at *www.oyez.org/cases/2000–2009/2006/2006_06_278/* (holding that the First Amendment rights of students in school and at school-supervised events are not as broad as those of adults in other settings).

[21] *Planned Parenthood of Cent. Mo.* v. *Danforth*, 428 U.S. 52, 74 (1976) (minors' right to abortion). *See also Bellotti* v. *Baird*, 443 U.S. 622, 635 n.13 (minors possess close to the "full capacity for individual choice which is the presupposition of First Amendment guarantees"); Catherine Ross, *An Emerging Right for Mature Minors to Receive Information*, 2 U. PA. J. CONST. L. 223 (1999); Lee Tien & Seth Schoen, Reply Comments of the Electronic Frontier Foundation filed in *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*, MB Docket No. 0926, Federal Communications Commission, May 18, 2009, *http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520216901.*

[22] *See generally* Solveig Singleton, Privacy Versus the First Amendment: A Skeptical Approach, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97 (2000), available at *http://law.fordham.edu/publications/articles/200flspub6588.pdf*; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1175 (2000), available at *www.law.ucla.edu/volokh/privacy.htm.*

[23] "There are parents who, for a variety of reasons (political, cultural, or religious beliefs, ignorance of the facts, fear of being exposed as abusers, etc.), would deliberately prevent their teens from accessing social-network sites (SNS)." Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States,* Dec. 31, 2008, Appendix F, Statement of Connect Safely, at 262, *http://cyber.law.harvard.edu/pubrelease/isttf* (listing examples of unintended consequences of age

Continued

Preserving the ability of adolescents to participate in online interactions goes beyond content that most people would recognize as "serious"—from the perspective of both First Amendment values and the education of children. As a recent MacArthur Foundation study of the youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[24]

Even if parents have an absolute right to block their adolescents' access to such data, they can better exercise that right by applying strict controls on the computers in their home. As discussed below, there are ways to encourage innovation in such parental empowerment tools without changing COPPA itself. But COPPA 2.0 proposals go well beyond recognizing parents' rights by making parental consent a "default" requirement for adolescents to access a wide range of content—meaning that parents must "opt-in" on behalf of their children before their children can participate in sites and services covered by COPPA. This, in turn, burdens the ability of adolescents to communicate, because their parents might censor (rightly or wrongly) certain information, or simply fail to understand the technologies involved or be responsive to the opt-in requests when their kids want to access a new interactive site or service. But whatever the free speech rights of adolescents, if anyone should be interfering with those rights, it should be their parents—not the government.

2. COPPA's Current Age Range Allows Beneficial Communication between Adolescents and Adults

Finally, COPPA 2.0 could infringe on the free speech rights of adults to communicate with adolescents online by driving operators to segregate users by age or to attempt to block access by adolescents. As explained below, for the sake of marginal (if any) gains in child protection, we would be excluding *beneficial* interaction between adults and minors.

The vast majority of online interactions between adults and minors are not of a harassing, predatory or otherwise harmful nature—indeed, they generally involve adults looking to help or assist minors in various ways. As the MacArthur Foundation study cited above concluded:

> In contexts of peer-based learning, adults . . . have an important role to play, though it is not the conventionally authoritative one. In friendship-driven practices, direct adult participation is often unwelcome, but in interest-driven groups we found a much stronger role for more experienced participants to play. Unlike instructors in formal educational settings, however, these adults are passionate hobbyists and creators, and youth see them as experienced peers, not as people who have authority over them. *These adults exert tremendous influence in setting communal norms and what educators might call "learning goals," though they do not have direct authority over newcomers.*[25]

A substantial portion of those interactions involve parents talking to their own kids, older and younger siblings communicating with one another, teachers and mentors talking to their students, or even co-workers of different ages communicating. Even when adult-minor communications involve complete strangers, there is typically a socially-beneficial purpose. Examples include debating politics on a discussion board, or collaboratively editing a Wikipedia entry, or communicating and collaborating on a common purpose on a Presidential campaign website involving millions of volunteers of all ages. There are countless other examples. Such interactions could be severely curtailed by COPPA 2.0 proposals. Restricting such interactions would raise profound First Amendment concerns about freedom of speech as well as of association.

In any First Amendment analysis, a court must consider not only the free speech rights at stake and the availability of less restrictive alternatives to regulation, but the governmental interest being advanced. Again, neither COPPA nor the COPPA 2.0 proposals recently contemplated at the state level require exclusion of older users from a website, nor directly govern the sharing of personal information among

---

verification mandates) [hereinafter *ISTTF Final Report*]. Full disclosure: Adam Thierer was a member of this task force.

[24] John D. and Catherine T. MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, at 2 [hereinafter *MacArthur Study*] *http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf*.

[25] *MacArthur Study, supra* note 24, at 2.

users (where that sharing does not also constitute collection by the site itself). But separation of adolescents from adults is likely to be an indirect effect of COPPA 2.0 requirements—as COPPA 2.0 advocates probably realize—because, once operators are required to age-verify users, they will face reputational, political and potentially legal pressure to make interactions between adolescents and children more difficult in the name of "child safety." More subtly, if site operators have an incentive to avoid having their sites be considered "directed at" adolescents, they will also have an incentive to discourage adolescent participation on their sites—which achieves a similar result.

Given the lack of strong identity records for minors, it's much easier for an adult to pretend to be a minor than vice versa. Thus, one must further ask if attempting to quarantine children from adults (however indirectly) actually advances, on net, a strong governmental interest in child protection. Such a quarantine is unlikely to stop adults with truly nefarious intentions from communicating with minors, as systems designed to exclude participation by adults in a "kids-only" or "adolescents-only" area can be easily circumvented. The effect of age stratification on truly bad actors is likely to be marginal at best—or harmful at worst: Building walls around adolescents through age-verification might actually make it *easier* for predators to target teens, since a predator who gains access to a supposedly teen-only site will be less likely to be exposed as a predator than by targeting an adult the predator thinks is a teen.

To hear some of the advocates of COPPA expansion talk about how teens currently behave online, one might think that online environments in which adolescents were left to their own devices—imagine a "Teen MySpace" for the 13–17 crowd, walled off from the rest of MySpace—would be far worse, perhaps an online version of *Lord of the Flies*. These concerns are clearly exaggerated: The critics frequently complain about "the way kids talk to each other these days" while looking at their own past adolescent banter with rose-tinted glasses. What is clear is that adolescents (and young adults) behave *better* in online environments where adults are present, too. Perhaps the best demonstration of this fact has been the uproar from adolescents and young adults that has accompanied Facebook's explosive growth in popularity among older users.[26] Many kids hate the idea of adults joining Facebook precisely because the presence of adults encourages kids to "self-regulate" by exercising better judgment and following better netiquette.[27]

Anne Collier, founder and executive director of the child safety advocacy organization Net Family News, Inc. and editor of NetFamilyNews.org and ConnectSafely.org, suggests that the push for "segregation" by age (*e.g.,* creating a teen-only version of Second Life) for safety's sake is "losing steam" because:

> It's a response to the predator panic teens and parents have been subjected to in U.S. society, not to the realities of youth on the social Web. What nearly a decade of peer-reviewed academic research shows is that peer-to-peer behavior is the online risk that affects many more youth, the vast majority of online kids who are not already at-risk youth offline. Segregating teens from adults online doesn't address harassment, defamation, imposter profiles, cyberbullying, etc. It may help keep online predators away from kids (even though online predation, or abuse resulting from online communication, constitutes only 1 percent of overall child sexual exploitation . . .), which is a great outcome, but it's not enough unless all that parents are worried about is predators.[28]

Of course, adults play a critical role in disciplining interaction among the 0–12 age bracket, but not as direct participants in on-site interaction. Again, how many

---

[26] Justin Smith, *Number of U.S. Facebook Users Over 35 Nearly Doubles in Last 60 Days*, Inside Facebook Blog Mar. 25, 2009, *www.insidefacebook.com/2009/03/25/number-of-us-facebook-users-over-35-nearly-doubles-inlast–60-days/*.

[27] *See e.g.,* Lori Aratani, *When Mom or Dad Asks To Be a Facebook "Friend,"* THE WASHINGTON POST, Mar. 9, 2008, *www.washingtonpost.com/wp-dyn/content/article/2008/03/08/AR2008030801034.html*. "'I do not know if this has happened to anybody, but this morning I log on to Facebook and I have a new friend request!' wrote 19-year-old Mike Yeamans, a sophomore at James Madison University, on one of several 'No Parents on Facebook' groups that have popped up on the site. 'I am excited to make a new friend so I click on the link. I could not believe what I saw. My father! This is an outrage!'" *Id.*

[28] Anne Collier, *Where Will OnlineTeens Go Next?,* May 1, 2009, *www.netfamilynews.org/2009/05/where-will-online-teens-go-next.html* (internal citations omitted). For evidence of at-risk youth, Collier sites the *ISTTF Final Report, supra* note 47. Regarding the percentage of all child sexual exploitation that results from online communication, she cites Janis Wolak, David Finkelhor & Kimberly Mitchell, Crimes Against Children Research Center, Trends in Arrests of Online Predators, 2009) *www.unh.edu/ccrc/pdf/CV194.pdf; see also*, Anne Collier, *Major Update on Net predators: CACRC study*, March 31, 2009, *www.netfamilynews.org/2009/03/majorupdate-on-net-predators-mostly.html* (summarizing study).

adults actually want to use Club Penguin, a site clearly geared toward the Net's youngest users? Instead, parents can supervise what their kids do online through parental control software. Parents could, of course, use that same software to monitor what their adolescent kids do, too. But as kids get older, most parents realize that the training wheels have to come off at some point. Few parents will want to spy on their 17-year-old until the day before the kid starts college (or enlists in the military or gets married). But most parents probably *would* prefer that, if their kids are interacting in an online environment, they think twice about what they do and say online. It is by no means clear that restricting online interaction between teens and adults will serve that end.

B. Do you think COPPA should be strengthened?

I have seen no evidence of a need for Congress to reopen COPPA, and to the extent that some changes may be necessary in the implementation of COPPA, I believe the statute affords the FTC great flexibility in its definition of "Internet," as discussed below, as well as in allowing the agency to update the definition of "personal information." Thus, while there may be ways to improve implementation of the statute, I do not see a need for changing COPPA itself today.

Moreover, Congress must be cognizant of the downsides of reopening COPPA and—to the extent it is expanded along the lines some of have advocated—raising the prospect of the entire law being struck down as unconstitutional because it essentially converges with COPA, as Adam Thierer and I have explained in our work.[29] Again, COPPA is one of the few Internet laws Congress has passed over the last 15 years that was not challenged, blocked from taking effect, or overturned.

C. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

As I noted in my testimony, COPPA already gives the FTC the flexibility to update the definition of "personal information" to include "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[30] Because the definition of personal information also includes "information concerning the child or the parents of that child that the website collects online from the child and combines with [any of these identifiers]," the statute already covers essentially all information tied to a particular user where it is possible to contact that user. This dynamic definition is broad enough to keep pace with technological change because it is not simply a static listing of the "personal information" that was at issue in the late 1990s. For example, if the lodestar of "personal information" is the ability to contact a child, instant messaging screen names or social networking pseudonyms might qualify as "personal information." In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

The biggest threat to children's online privacy and safety has always been, and will likely remain, the ignorance and naïveté that necessarily comes with youth. Though children may be quite technologically adept, far more so than many parents, they still lack the real-world experience necessary to appreciate the potential privacy and safety implications of heedlessly giving personal information away to site operators or, especially, making personal information publicly available to other Internet users. No amount of Federal legislation or regulation is going to keep children from divulging personal information if they aren't aware of its dangers. So, as discussed below, if a lack of knowledge or sophistication is the problem, the primary answer must be education, education and more education, not regulation, regulation, and more regulation.[31]

D. What do you think is the most urgent update to COPPA needed?

Again, the FTC should remove any doubt about the fundamental technological agnosticism of COPPA's potential coverage (actual coverage depending on whether, in any particular context, "collection" occurs and whether the site is directed at children or the operator has actual knowledge that it is "collecting" personal information from a child). The FTC should also encourage the development of mechanisms for verifying parental consent appropriate to these technologies, either by recognizing additional mechanisms or through certifying innovative safe harbor operators. Congress could direct, and fund, the FTC to conduct more education about COPPA, online privacy and online safety.

---

[29] *See generally supra* note 2.
[30] 15 U.S.C. § 6501(8)(F).
[31] *See infra* at III.A.4.

E. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

COPPA already includes an excellent list of personal information:

(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;[32]

As I noted in my testimony, COPPA already gives the FTC the flexibility to update the definition of "personal information" to include "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[33] Because the definition of personal information also includes "information concerning the child or the parents of that child that the website collects online from the child and combines with [any of these identifiers]," the statute already covers essentially all information tied to a particular user such that it is possible to contact that user. Thus, there should be no need to specify additional categories of sensitive data to achieve COPPA's purposes.

F. You said in your written testimony that a "COPPA expansion would undermine privacy." Would you mind explaining to the Committee your meaning?

Sites that implement age verification technologies (even through COPPA's "verifiable parental consent" loose form of age verification) require users to share personal information about themselves. Specifically, adults attempting to access sites behind an age verification wall would have to provide information adequate to establish that they are not, in fact, younger than whatever the higher age threshold of COPPA 2.0 might be. Similarly, children attempting to access such sites would have to provide information about themselves and their parents sufficient to establish the parent-child relationship so that a site can reasonably evaluate documentation purporting to establish "verifiable parental consent." Both forms of age verification (by adults, and by children/parents) could be accomplished by a number of means, but seem to be most commonly done today through use of a credit card.

Today, because COPPA requires age verification only for sites "directed at" children under 13 (or, in cases where an operator has "actual knowledge" that a particular user is under 13), the law in practice requires only the second sort of age verification. But if COPPA were expanded to cover, say, all sites "directed at" adolescents (however defined), the law would very likely require certain website operators to presume that *all* their users might be "children" whose parents' "verifiable parental consent" must be obtained prior to collection. This, in turn, would mean that large numbers of adults would, for the first time since COPA, be required by law (or at least, the website operator's interpretation of the law, which might tend to err on the side of caution) to age verify significant numbers of adults. As discussed below, this creates a significant burden on the First Amendment rights of adults to anonymous communication through interactive services that could allow public sharing of personal information. This would also significantly burdens website operators whose audience might be reduced by the apprehension caused by age verification mandates among users worried about having to provide information for certification purposes or simply by the hassle of having to do so. In both respects, COPPA 2.0 would raise precisely the same constitutional problem that caused the courts to strike down COPA (but that are not raised by COPPA 1.0).[34]

But such an expansion of COPPA's age scope would also undermine privacy by requiring the sharing of more personal information in order to age-verify newly covered users. The same would be true of any attempts to expand COPPA by specifying that it applies to certain categories of websites (effectively disposing of the law's "directed at" analysis). *Thus, the irony of COPPA expansion is that lawmakers would be applying a law that was meant to protect the privacy and personal information of children to gather a great deal more information about kids, their parents, and many other adults.*

As the district court that struck down COPA noted:

> Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material

[32] 15 U.S.C. § 6501(8)(A–E).
[33] 15 U.S.C. § 6501(8)(F).
[34] *See supra* at 3–9.

> privately and anonymously, especially if it is sexually explicit. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.[35]

The same is true even for non-explicit material, such as would be covered by COPPA if the law's age range were expanded.

G. Do you support the FTC's review of COPPA? Do you believe it is necessary?

Yes, the FTC was well within its general operating procedures to accelerate its review of the COPPA Rules from 2015, the originally set date, to this year,[36] and it made sense for the agency to do so, given the pace of change in this area. In particular, it appears from comments made by many in industry that the FTC needs to do more to make clear that COPPA is, by original Congressional design, platform-agnostic, applying to any "collection" (including publication or sharing by users themselves) of "personal information" through a website or online service—*regardless of the device used to access that site or service.*

H. If you oppose expanding COPPA, do you believe it is working properly? Do you believe it is sufficient to protect children's privacy?

The original goals of COPPA, as expressed by its Congressional sponsors, were to:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[37]

Thus, as its name implies, COPPA is generally concerned with protecting the privacy of children. But COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools . . . for becoming involved in and overseeing their children's interactions online."[38] However admirable, "protect[ing] the safety of children" is merely an *indirect* goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's *direct* goal).

Viewed in this light, COPPA has probably been about as successful as could be expected given the fundamental technical reality of the Internet: In general, users and operators cannot, across the essentially infinite expanse of the digital chasm, definitively know how old other users are or even who they are.

The FTC asserts COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[39] Yet many of those advocating expansion of COPPA do so on the grounds that COPPA makes children safer from sexual predators. What these advocates fail to acknowledge is that, to the extent COPPA has enhanced child safety—indeed, to the extent that COPPA can be effectively administered at all—it is because of the unique circumstances of the under–13 age bracket and the operators that have evolved to serve that community. In particular:

> 1. The functionality of child-oriented sites is usually tightly limited: They are walled gardens;
>
> 2. Many smaller websites catering to children charge a fee for admission—even as fee-based models have withered away on the rest of the Internet; and
>
> 3. There are relatively few sites that cater exclusively to the under–13 crowd, which may be an unintended consequence of COPPA itself.

---

[35] *Gonzales*, 478 F. Supp. 775, 805 (E.D. Pa. 2007).

[36] *See* Federal Trade Commission, Staff Report, *Beyond Voice: Mapping the Mobile Marketplace*, April 2009, at 3, *www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf*; *see also* FTC Operating Manual, § 7.5, at 33, *http://www.ftc.gov/foia/ch07rulemaking.pdf* (The FTC "has adopted a policy of reviewing each of its legislative rules (*i.e.,* trade regulation rules and rules promulgated under special statutes) at least once every 10 years.").

[37] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[38] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 28, Feb. 2007, *www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf* (2007 COPPA Implementation Report).

[39] *Id.* at 28.

I. Would you support any changes to the rule or to the statute?

I would support changes to the statute if:

1. It were shown that those changes were necessary to prevent a demonstrable and substantial harm (not just a fear of potential harm), were narrowly tailored to that harm, and were the least restrictive means available for addressing that harm;

2. Those changes could reduce the difficulty and expense of complying with COPPA, thus promoting competition in the marketplace for children's content and services; or

3. Those changes could further empower parents to make decisions about their children's participation in online sites and services, without unduly burdening those sites and services.

But as explained throughout, I believe the FTC already has the tools it needs under COPPA in its current form. If the FTC needs anything more from Congress, it might be additional funding for educational efforts, encouraging new safe harbor programs, and targeted enforcement.

II. Privacy Implications of New Technologies

A. You said in your written statement, "the reality is that the technology for reliable age verification simply doesn't exist." Could it exist in the future? If your claim is valid, does that mean the business community, the FTC or Congress should not strive to find enhanced age verification methods?

In a February 2007 report to Congress about the status of COPPA and its implementation, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online."[40] In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof."[41] The FTC attempted to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[42] This makes it clear that the FTC does not regard the methods the agency has prescribed for obtaining parental consent under COPPA as equivalent to strict age verification.

After years of searching for a technological "silver bullet," especially by state attorneys general, the practical limitations and dangers of age verification mandates are now widely recognized. Few continue to argue for directly mandating verification of the age of minors online—or that such verification, in its strictest sense, is even technically feasible. Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of websites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[43] Few public data bases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that do exist about their children (*e.g.,* birth certificates, Social Security numbers, school records) to become more easily accessible.[44] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[45]

There are a host of other concerns about age verification mandates.[46] Some of these concerns were summarized in a recent report produced by the Internet Safety

[40] *Id.*, at 1.
[41] *Id.* at 13.
[42] *Id.* at 12.
[43] *Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007).
[44] *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion,* PFF Blog, Sept. 25, 2008, *http://blog.pff.org/archives/2008/09/age_verificatio_1.html*.
[45] Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html*.
[46] For a fuller exploration of these issues, see Adam Thierer, The Progress & Freedom Foundation, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Progress on Point No. 14.5, Mar. 2007; Adam Thierer, The Progress & Freedom Foundation, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General*, Jan. 14, 2008, *www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf*;

Continued

Technical Task Force, a blue ribbon task force assembled in 2008 by state attorneys general to study this issue:

> Age verification and identity authentication technologies are appealing in concept but *challenged in terms of effectiveness*. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.[47]

But even if far more robust age verification solutions could be developed, they would not solve the central constitutional problem faced by efforts to expand COPPA's age range or scope of sites otherwise covered by COPPA regardless of age. This is because, in essence, the practical challenge under COPPA is not that children have to prove that they are in fact *under* a certain age, but two far more complicated problems.

First, once the verifiable parental consent requirement is triggered, either because a site is "directed at" children or because the operator knows that a particular user is a child (for example, because they have volunteered the fact that they are under 13 years old), the operator must make a "reasonable effort (taking into consideration available technology)" to verify parent-child relationship to ensure that adequate notice is given to, and authorization is obtained from, someone who is in fact the parent of that child.[48] This is more complicated than simply verifying the age of any particular user, and the statute's flexibility in exactly how operators are to fulfill this requirement is indicative of the difficulty involved.

Second is the very different problem of trying to ensure that a particular user is *not* a child. This is essentially the problem faced by COPA, where the solution was simply to require certain kinds of websites to age verify all users. Again, that solution is clearly unconstitutional, even though the material at issue was that deemed "harmful to minors" (increasing the government's interest in regulating communications). COPPA's ingenious way of sidestepping this problem is to limit broad verification mandates to sites that are "directed at" children or to situations where the operator has "actual knowledge" that a user is a child. (Furthermore, the verification required by COPPA is fundamentally different, being verification of "verifiable parental consent" rather than of the actual identity or age of a user.) This difference is profound, because it means that COPPA, in its present form, does not subject significant numbers of adults to age verification mandates. But, again, if the COPPA framework were expanded to cover older children or certain websites based on their functionality, COPPA would essentially converge with COPA by requiring large numbers of users to prove a negative: that they are *not* children.

It is difficult to see how that problem can ever be solved because even if there were a reasonably reliable solution for authenticating a user's identity, the constitutional analysis does not hinge on the accuracy of age or identity verification mechanisms, but on the chilling effects caused by government mandates that users provide more information about themselves than they otherwise would have to do in order to access certain interactive sites or services (that could potentially allow sharing of personal information). Simply put, this does not appear to be a problem that can be solved by any amount of technological innovation.

III. Policy Recommendations

A. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

1. The FTC Should Clarify COPPA's Technological Breadth

As noted above, the FTC should remove any lingering doubt that COPPA is platform-agnostic. While new technologies may indeed present unique challenges and opportunities for "enhancing parental involvement" in the online activities of children, it should be uncontroversial and clear to everyone that COPPA applies to any

---

Nancy Willard, *Why Age and Identity Verification Will Not Work—And is a Really Bad Idea*, Jan. 26, 2009, *www.csriu.org/PDFs/digitalidnot.pdf;* Jeff Schmidt, *Online Child Safety: A Security Professional's Take,* The Gardian, Spring 2007, *www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.*

[47] *ISTTF Final Report, supra* note 23, at 10.

[48] *See* 16 C.F.R. § 312.1 (definition of "Obtaining verifiable consent").

technology that facilitates the "collection" of personal information over the Internet (which, again, means not only collection by operators for advertising or other purposes but also simply enabling users to make personal information publicly available). This is simply the plain reading of the statute. COPPA defines the key term "Internet" broadly to mean:

> collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide 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.[49]

In its 1999 COPPA rulemaking, the Commission declared that:

> The proposed Rule's definition of "Internet" made clear that it applied to the Internet in its current form and to any conceivable successor. Given that the technology used to provide access to the Internet will evolve over time, it is imperative that the Rule not limit itself to current access mechanisms.[50]

The Commission rejected a commenter's suggestion that the agency "clarify that the definition 'clearly includes networks parallel to or supplementary to the Internet such as those maintained by the broadband providers . . . [and] intranets maintained by online services which are either accessible via the Internet or have gateways to the Internet.'" The Commission concluded that its "definition of 'Internet' was [already] sufficiently broad to encompass such services and adopts that definition in the final Rule.[51] The Commission has subsequently incorporated this language into its FAQ, which serves as its primary interpretive guide for those interested in understanding application of the rule (especially small site operators):

> The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.[52]

As a matter of statutory construction, this interpretation is probably correct and would probably receive deference from a court under the *Chevron* doctrine if challenged.[53] This interpretation would allow the FTC to apply COPPA's requirements to services like text messaging and Massively Multiplayer Online (MMO) games like World of Warcraft and Second Life that are "accessible via the Internet," regardless of the device used to access them.

2. The FTC Should Promote Flexibility in COPPA Compliance

The FTC should take into consideration the unique challenges and opportunities raised by new devices and services in deciding how to implement COPPA. Alternative means of establishing verifiable parental consent may work much better for the technologies, devices, and services of tomorrow, and the FTC will probably hear in great detail about this issue at its roundtable and in comments filed in response to its Implementation Review. In deciding how to respond to those suggestions, the FTC should aim to maximize the flexibility available to online operators to comply with COPPA, and to simplify the process wherever possible for parents and children. Where parents have already given effective consent for their children to use a particular service—for example, by paying for a text message plan as part of the monthly service for a cell phone—there may be no need to impose additional requirements because COPPA's goal of "enhancing parental involvement" through parental consent has already been achieved. More granular controls (say, blocking texting to a particular number) may be quite valuable to parents but they are probably beyond the purview of COPPA and, in any event, are already being offered by many service providers in response to parental demand.[54] This suggests the market-

---

[49] 15 U.S.C. § 6501(6).

[50] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 (Nov. 3, 1999), available at *www.ftc.gov/os/1999/10/64fr59888.pdf*.

[51] *Id.*

[52] Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, Question 6 ("What types of online transmissions does COPPA apply to?"), *www.ftc.gov/privacy/coppafaqs.shtm*.

[53] *Chevron U.S.A., Inc.* v. *Natural Res. Defense Council, Inc.,* 467 U.S. 837 (1984) (required Federal courts to defer to an agency's interpretation of a statute, so long as the interpretation was "reasonable").

[54] *See, e.g.*, Verizon Wireless, Usage Controls, *https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_home.jsp* (describing parental control tools available to parents including blocking num-

Continued

place is already working to empower parents, which is, after all, COPPA's primary purpose.

In particular, the FTC could use the discretion afforded to it by the statute to certify more "safe harbor" operators, whose self-regulatory guidelines would be deemed to be sufficient to establish compliance with COPPA. For example, as children under 13 increasingly have their own ever more sophisticated mobile phones,[55] wireless carriers and mobile operating system developers might collaborate on a standardized system that requires verifiable parental consent upon the initial purchase of a mobile phone service plan or addition of certain options, like text messaging or data service but that also provides parents control over which applications their children install on their phones. Such a system might work by, for instance, giving parents a password-protected account upon the initial verification of their consent for the service plan, and then allowing them to easily grant consent for their children to install applications in the future, keep track of those applications for which they have already granted consent, access information collected by those applications, review the privacy policies of those applications, or revoke their consent as they see fit. Such a system is, at least in theory, exactly what policymakers should aim to enable, but it may should be *required* by COPPA. The ultimate goal should be to encourage companies to empower parents to manage, as easily as possible, their children's participation in online activities that could entail the sharing of personal information—which is what parents are already demanding in the marketplace. But such a highly complex system should be designed and managed by the private sector, not the government, and this is precisely what the safe harbor program provided for by COPPA would allow the FTC to do to the extent consistent with COPPA's scope.

Concretely, lawmakers might encourage the FTC to issue a call to industry for new safe harbor proposals, to work with industry to support the development of these proposals, and then perhaps issue a consolidated notice about these proposals in order to expedite the notice and comment process required by the statute before the agency may grant approval to any new safe harbor program. More such suggestions will, no doubt, come out of the COPPA Roundtable and comments, and Congress should encourage the FTC to heed such suggestions.

Or, the FTC could, as the Implementation Review contemplates, allow operators, at least in some circumstances, to use "an automated system of review and/or posting" to satisfy the existing "deletion exception to the definition of collection."[56] In other words, sites could potentially allow children to communicate with each other through chat rooms, message boards, and other social networking tools *without* having to obtain verifiable parental consent if they had in place algorithmic filters that would automatically detect personal information such as a string of seven or ten digits that seems to correspond to a phone number, a string of eight digits that might correspond to a Social Security number, a street address, a name, or even a personal photo—and prevent children from sharing that information in ways that make the information "publicly available." Such a technology would, of course, not be foolproof, and might be circumvented by children smart enough to find other ways to share information that the algorithm will prevent them from sharing. Yet despite these limitations, the FTC should encourage the development of such technologies because they could allow sites to meet COPPA's central goal of limiting the sharing of information that could allow the contacting or identification of a child *without* going through COPPA's intentionally (or at least, necessarily) cumbersome parental consent verification procedures. This would benefit kids and operators alike by facilitating communication with less risk to children's online privacy or safety.

3. Enhanced Enforcement Is Generally Preferable to Expanded Regulation

Besides promoting empowerment solutions, the FTC should of course be vigilant about a second "E-word": *enforcement*. As a general matter, before rushing to change an existing regulatory regime or give an agency new powers, Congress should always ask whether the laws on the books are being given a chance to succeed. Specifically, Congress should consider whether the FTC has the staffing, technological and financial resources it needs to enforce COPPA's requirements effectively.

---

bers, time restrictions and usage filters); *https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_content_filter.jsp* (content filters); *see generally http://parentalcontrolcenter.com/#_self; http://www.wireless.att.com/learn/articles-resources/parentalcontrols/index.jsp; http://shop.sprint.com/en/services/safety_security/parental_control.shtml*.

[55] Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, *Teens and Mobile Phones*, April 20, 2010, *http://www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones.aspx*.

[56] COPPA Implementation Review, *supra* note 5, Question 9a.

4. Education is Vitally Important

Finally, the FTC should be encouraged—and funded—to make maximum use of the final "E-word": *education*. We can and should provide parents with more and better tools to make informed decisions about media and communications tools in their lives and the lives of their children. But technical tools can only supplement—they can never supplant—education, parental guidance, and better mentoring. Education and mentoring are the most essential part of the solution to concerns about online child privacy and safety. We can, and must, do more as parents and as a society to guide our children's behavior and choices online. The FTC has a track record of great success in this area, including:

- OnGuard Online, the website intended to educate all Internet users about online safety
- NetCetera, the FTC's excellent child safety effort
- The "You Are Here" virtual mall launched by the FTC last year to educate kids in 5th–8th grade (ages 10–14) about marketing both online and offline.
- AdMongo, a game-tutorial website intended to teach kids about advertising and marketing, both online and offline, to help them become smarter consumers. The service includes a discussion of how information is used for advertising purposes online.

In addition, Congress could fund a number of grants for educational efforts intended to educate kids and parents about online privacy and safety. This approach is exemplified by Rep. Wasserman Schultz's currently pending "Adolescent Web Awareness Requires Education Act (AWARE Act)" (H.R. 3630), which would create a education grant program to address issues of cybercrime affecting children, including cyber bullying, in schools and communities.[57] Indeed, The "Protecting Children in the 21st Century Act," which was signed into law by President Bush in 2008 as part of the "Broadband Data Services Improvement Act,"[63] required that the Federal Trade Commission (FTC) "carry out a nationwide program to increase public awareness and provide education" to promote safer Internet use and:

> utilize existing resources and efforts of the Federal Government, State and local governments, nonprofit organizations, private technology and financial companies, Internet service providers, World Wide Web-based resources, and other appropriate entities, that includes: (1) identifying, promoting, and encouraging best practices for Internet safety; (2) establishing and carrying out a national outreach and education campaign regarding Internet safety utilizing various media and Internet-based resources; (3) facilitating access to, and the exchange of, information regarding Internet safety to promote up to-date knowledge regarding current issues; and, (4) facilitating access to Internet safety education and public awareness efforts the Commission considers appropriate by States, units of local government, schools, police departments, nonprofit organizations, and other appropriate entities.

Education-based approaches are vital because they can help teach kids how to behave in—or respond to—a wide variety of situations. Education teaches lessons and builds resiliency, providing skills and strength that can last a lifetime. That was the central finding of a blue-ribbon panel of experts convened in 2002 by the National Research Council of the National Academy of Sciences to study how best to protect children in the new, interactive, "always-on" multimedia world. Under the leadership of former U.S. Attorney General Richard Thornburgh, the group produced a massive report that outlined a sweeping array of methods and technological controls for dealing with potentially objectionable content and online dangers. Ultimately, however, the experts used a compelling metaphor to explain why education was the most important strategy on which parents and policymakers should rely:

> Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment

[57] Adolescent Web Awareness Requires Education Act, H.R. 3630, 111th Cong. (2009), available at www.opencongress.org/bill/111-h3630/show.

about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify.[58]

Regrettably, we often fail to teach our children how to swim in the "new media" waters. Indeed, to extend the metaphor, it is as if we are generally adopting an approach that is more akin to just throwing kids in the deep end and waiting to see what happens. Educational initiatives are essential to rectifying this situation.

B. Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?

It's still probably too early to say with any certainty what that direction is—especially on the eve of the FTC's COPPA Roundtable. In general, I am encouraged by the tone of the FTC's official statements in this proceeding, and also by the oral statements of FTC staff at recent events. They appear to have a healthy understanding of the limitations as well as the advantages of COPPA, as well as a healthy sensitivity to the potential effects on the competitiveness of the landscape for children's content and services.

I'm particularly encouraged to see that the implementation review begins by asking about the ongoing need for the rule, its costs and benefits, and its unintended effects. This is precisely the right way to begin any inquiry into the implementation of regulations. COPPA has undoubtedly succeeded in its primary goal of enhancing parental involvement in their child's online activities in order to protect the privacy and safety of children online.[59] Yet these benefits have come at a price, since the costs of obtaining verifiable parental consent and otherwise complying with COPPA have, on the one hand, discouraged site and service operators from allowing children on their sites or offering child-oriented content, and, on the other hand, raised costs for child-oriented sites. The average cost of compliance may well have fallen from the estimate provided to the FTC in 2005 ($45/child),[60] but even substantially lower costs on the order of $5–10 per child could represent a significant barrier to entry by sites that must rely, as most online sites and services do, on advertising revenues of scarcely more than that—and profit margins far less than that—per user per year. We must be realistic about these costs and the trade-offs involved in regulation. At some point, raising the cost of age verification for sites is simply no longer worth the marginal benefit to enhanced parental involvement and, indirectly, online child privacy and safety, because these values must compete with other values of parents and children, such as the competitiveness, creativity, innovation and diversity in media and tools available to children online. COPPA in its current form probably strikes a reasonable balance, but as noted above, there may indeed be things that the FTC can do to lower the costs of compliance for operators, thus allowing us to achieve COPPA's goals at a lower cost to kids and parents in foregone content and services. I am also pleased that the Implementation Review asks about the need to update the "sliding scale" of parental consent verification methods and to offer greater flexibility to site operators, as noted above.

But I do worry that the Commission has explicitly invited proposals for legislative changes to the statute itself. Two questions from the Review are particularly troubling:

> *6.* Do the definitions set forth in Part 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety? . . .
>
> *28.* Does the commenter propose any modifications to the Rule that may conflict with the statutory provisions of the COPPA Act? For any such proposed modification, does the commenter propose seeking legislative changes to the Act?

Note that question #6 does *not* include the critical limitation "consistent with the Act's requirements," which appears no less than 17 times in subsequent questions about specific aspects of the current rules. Whatever the FTC intended by this omission, when combined with question #28, it will be taken as an open invitation by many commenters to propose not just changes in how the COPPA rules are implemented, but wholesale revisions to the COPPA statute itself.

Ultimately, it is the responsibility of Congress, not the FTC, to make decisions about modifying the statute. If Congress wants an agency to spend taxpayer re-

---

[58] Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (National Academy Press, 2002) at 224, *www.nap.edu/openbook.php?isbn=0309082749&page=224*.

[59] *See COPPA 2.0, supra* note 2 at 11.

[60] *See* Comments of Parry Aftab, *Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children* at 2, June 27, 2005, *www.ftc.gov/os/comments/COPPArulereview/516296–00021.pdf*.

sources evaluating whether a substantial change to the agency's statutory authority is warranted, Congress is perfectly capable of authorizing, and appropriating funds for, such an inquiry. This is precisely what Congress recently did in the Child Safe Viewing Act, when it specifically asked the Federal Communications Commission (FCC) to prepare a report on online child safety issues.[61] Similarly, the Recovery Act of 2009 charged the FCC with preparing a national broadband plan.[62] Or, where less substantial statutory changes are at issue, the Congressional Committee with jurisdiction could request that an agency prepare a report to advise that committee. But as a general matter, regulatory agencies should not be in the business of reassessing the adequacy of their own powers, since the natural impulse of all bureaucracy is to grow, and it is through our elected representatives in Congress, not regulatory agencies—even those with the best of intentions—that "We People" are ultimately represented in deciding how to regulate the online (and offline) world.[63]

Finally I was surprised not to find a single mention of the word "education" in the FTC's Implementation Review Request for Comments. As explained above, just about everyone involved in debates about online child safety and privacy would agree that the solution begins with education—even if it doesn't end there. One might have thought the FTC would ask about whether effective implementation of COPPA's goals required more education efforts rather than (or perhaps in combination with) "stronger" regulations. Again, a layered approach of education, empowerment and enforcement is the best way to enhance the privacy and safety of children online, but education is truly the key.

Related PFF Publications

Written Testimony to the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Consumer Protection on "An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act", April 29, 2010.

COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech, Berin Szoka & Adam Thierer, Progress on Point 16.11, May 2009.

Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677, Berin Szoka, March 4, 2010.

Parental Controls & Online Child Protection: A Survey of Tools & Methods, Adam Thierer, Special Report, Version 4.0, Fall 2008.

Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer, Adam Thierer, Progress on Point 16.13, July 8, 2009.

The Perils of Mandatory Parental Controls and Restrictive Defaults, Adam Thierer, Progress on Point 15.4, April 11, 2008.

Written Testimony to House Committee on the Judiciary on Cyber Bullying and other Online Safety Issues for Children, Berin Szoka & Adam Thierer, Sept. 30, 2009.

Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech, Comments of Berin Szoka to FTC Exploring Privacy Roundtable, Nov. 2009.

Privacy Polls v. *Real-World Trade-Offs*, Berin Szoka, Progress Snapshot 5.10, Oct. 2009.

Online Advertising & User Privacy: Principles to Guide the Debate, Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.

Targeted Online Advertising: What's the Harm & Where Are We Heading?, Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.

How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight, Berin Szoka, Progress Snapshot 6.7, March 2010.

---

[61] Child Safe Viewing Act, S. 602, 110th Cong. (2007).

[62] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, 123 Stat. 115 (2009) (codified at 47 U.S.C. §1305) ("2009 Recovery Act"); *see also, A National Broadband Plan for Our Future*, GN Docket No. 09–51, Notice of Inquiry, 24 FCC Rcd. 4342 (2009) (*"NOI"*).

[63] *See, e.g.,* Super-Sizing the FTC & What It Means for the Internet, Media & Advertising, PFF Briefing, at 22–23, April 16, *www.pff.org/issues-pubs/pops/2010/pop17.6-transcript.pdf*.

ATTACHMENT

Do Smart Phones = Smart Kids?

THE IMPACT OF THE MOBILE EXPLOSION ON AMERICA'S KIDS, FAMILIES, AND SCHOOLS

A Common Sense Media White Paper

April 2010/*Common Sense Media*

Mobile technology is dramatically changing life for all of us, but especially for the earliest adopters of all things digital—our kids. Mobile phones and devices give kids many new opportunities for entertainment, engagement, and creativity, and make it easier to stay connected—including with mom and dad. Unfortunately, the 24/7 access-anywhere world of mobile also makes parenting even more complicated, and many adults worry about the growing challenge of managing the content, applications, and connections kids now have at their fingertips.

In 1983, the first cell phones weighed 28 ounces, measured 10 inches high, and sold for thousands of dollars. Today's mobile phones are often smaller than a deck of cards, weigh less than four ounces, and are often free as part of a one- or two-year contract. Increasingly, they offer touchscreens, GPS navigation, music, video, cameras, e-mail, and Internet browsing, not to mention the ability to download hundreds of thousands of applications and games.

In 1985, there were about 200,000 cell phone subscribers in the United States. Today, there are more than 286 million subscribers,[1] and nearly nine in 10 (87 percent) Americans own a cell phone.[2] More than 50 million of them own smartphones and wireless enabled PDAs.[3] In addition, purchases of WiFi-enabled devices such as cameras, game players, and media players, are expected to increase from 108 million in 2009 to 177 million in 2013.[4]

Increasingly, these handheld devices are becoming miniature computers, enabling users to access information and resources from anywhere. One sign of this change is the growth of mobile applications—2.3 billion apps were downloaded in the past year alone, and more than five billion will be downloaded per year by 2014.[5]

Mobile Kids

In 2004, 45 percent of teens had a cell phone; by 2009, it was 75 percent.[6] The fastest growth has been among younger teens:

- In 2004, just 18 percent of 12 year olds had a cell phone, compared to 64 percent of 17 year olds.
- In 2009, 58 percent of 12 year olds had a cell phone, compared to 83 percent of 17 year olds.[7]

Mobile phone usage is also growing rapidly among younger children. Twenty percent of U.S. children ages 6–11 currently own a cell phone, up from 11.9 percent of children in 2005.[8]

- U.S. teens (ages 13 to 17) send or receive an average of 3,146 text messages a month, and kids 12 and under send 1,146 texts per month.[9]
- More than a third of teens download ringtones, IM, or use the mobile web.
- About a quarter download games and applications.
- 16 percent use location-based services on their phones.[10]

---

[1] *http://www.ctia.org/media/press/body.cfm/prid/1936.*

[2] *http://www.marketingcharts.com/interactive/employment-age-top-factors-in-cell-phone-pda-use-9678/.*

[3] *http://www.ctia.org/media/press/body.cfm/prid/1936.*

[4] *http://www.instat.com/press.asp?ID=2694&sku=IN0904521WBB.*

[5] *http://news.softpedia.com/news/Five-Billion-Mobile-Apps-Downloaded-by–2014–130189.shtml.*

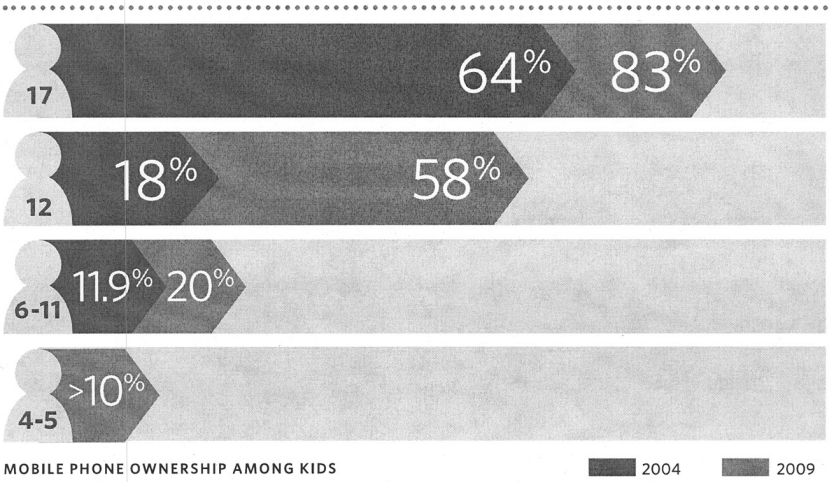
[6] *http://www.pewinternet.org/Reports/2009/14__Teens-and-Mobile-Phones-Data-Memo.aspx.*

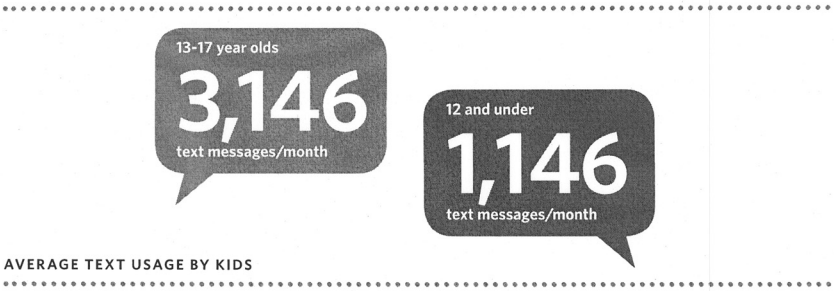
[7] *http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.*

[8] *http://www.npd.com/press/releases/press__080625.html.*

[9] *http://blog.nielsen.com/nielsenwire/online__mobile/under-aged-texting-usage-and-actual-cost/.*

[10] *http://blog.nielsen.com/nielsenwire/online__mobile/breaking-teen-myths/.*





Other Digital Devices

Most teens use computers to go online, but increasingly, they're also going online with their mobile devices.

- 27 percent of teen cell phone users use their phone to go online.
- 24 percent of teens with a game console (like a PS3, Xbox or Wii) use it to go online.
- 19 percent of teens with a portable gaming device use it to go online.[11]

Just over half of teens (51 percent) own a portable gaming device like a PSP or a Gameboy. Younger teens are more likely to have them (66 percent of 12–13 year olds, compared to 44 percent of 14–17 year olds).[12] Kids can use these devices to download TV shows and movies, surf the web, listen to music, and send instant messages.[13] Similarly, while the iPod Touch is not a smartphone, it enables users to text, access the web, and download apps. Sixty-five percent of iPod Touch users are 17 or younger.[14]

---

[11] *http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.*
[12] *http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.*
[13] *http://us.playstation.com/psp/fullfeatured/index.htm.*
[14] *AdMob—January 2010 Mobile Metrics Report. http://metrics.admob.com/.*

How Kids Are Using Mobile Tech

The Good News

A variety of recent studies have shown that integrating technology into schools can boost achievement in mathematics, literacy, and reading.[15]

- In four North Carolina schools in low-income neighborhoods, 9th- and 10th-grade students were given smartphones and special software to help with their algebra studies. They used the phones for a variety of tasks, including recording themselves solving problems and posting the videos to a private social networking site for their classmates. Students with the phones performed 25 percent better on the end-of-the-year algebra exam than students without the devices in similar classes.[16]
- A new study in the U.K. found that text messaging helped children develop "phonological awareness" which is key to learning how to spell. The kids who text more often (especially those who use abbreviations such as "plz" or "4ever") showed higher scores on spelling exams. Researchers also found that kids who received mobile phones at younger ages were better at reading words and identifying patterns of sound in speech.[17]
- Teachers in Escondido Union School District in California are exploring the use of iPods to improve student reading. Students can record and then hear themselves reading, which helps them work on fluency and comprehension. Teachers can import student recordings and create time-stamped digital portfolios to track progress. Data from a group of fourth-graders has found that using iPods to practice reading resulted in more rapid improvement rates compared with a control classroom.[18]

More generally, there are a number of ways that mobile devices can improve education:

- Mobile devices allow students to gather, access, and process information outside the classroom, and can help bridge school, afterschool, and home environments.
- Because of their relatively low cost, handheld devices can help level the digital playing field, reaching and inspiring children from economically disadvantaged communities.
- Mobile devices can support personalized learning experiences, and adapt to the individual needs of learners.[19]

The Bad News

Cyberbullying

43 percent of kids admit to being cyberbullied, but only 10 percent tell someone about it.

Cyberbullying is when someone repeatedly harasses, mistreats, or makes fun of another person online or while using cell phones or other electronic devices.

- Cyberbully 411 reports that 40 percent of kids say they were cyberbullied through instant messenger services; 30 percent said it happened on social networking sites; 29 percent said it happened while playing online games.
- Cyberbullying is especially prevalent in middle school-aged kids (9–14).[20]

Sexting

22 percent of teen girls (ages 13–19) say they have sent nude or semi-nude photos or video of themselves, either online or via text messages.

- Messages are even more prevalent than images. Thirty-nine percent of teen boys and girls say they have sent sexually suggestive messages (text, e-mail, IM), and 48 percent of teens say they've received them.
- Kids who sext may face criminal charges for child pornography or other violations, and could be required to register as sex offenders.[21]

---

[15] *http://www.iste.org/Content/NavigationMenu/Advocacy/Policy/59.08-PolicyBrief-F-web.pdf.*
[16] *http://www.nytimes.com/2009/02/16/technology/16phone.html?__r=1.*
[17] *http://www.britac.ac.uk/news/news.cfm/newsid/14.*
[18] *See Appendix A__http://www.joanganzcooneycenter.org/pdf/pockets__of__potential.pdf.*
[19] *http://www.joanganzcooneycenter.org/pdf/pockets___of__potential.pdf.*
[20] *http://www.commonsensemedia.org/protecting-kids-cyberbullying.*
[21] *http://www.thenationalcampaign.org/sextech/PDF/SexTech__Summary.pdf.*

Distracted Driving

In 2007, AAA reported that 21 percent of fatal car crashes involving teens between the ages of 16 and 19 were the result of cell phone usage.

According to the National Highway Traffic Safety Administration, in 2008 there were 5,870 fatalities and an estimated 515,000 injuries in police-reported crashes involving driver distraction, and the highest incidence of distracted driving occurs in the under–20 age group.[22]

- 34 percent of texting teens ages 16–17 say they have texted while driving.
- 52 percent of cell-owning teens ages 16–17 say they have talked on a phone while driving.[23]

Cheating

More than 35 percent of teens with cell phones admit to using their cell phones to cheat.

Kids have always found ways to cheat in school, but now they have more powerful tools.

- 45 percent of teens say texting friends about answers during tests is a serious cheating offense, but 20 percent say it's not cheating at all.
- 69 percent of schools have policies that don't permit cell use, but more than half of all kids ignore them.[24]

Location-Based Technology

Mobile phones with GPS capabilities can expose a kid's exact location. Many new programs and apps have been developed that allow kids to announce their physical whereabouts. This creates physical safety concerns.

If a kid shares location info to "friends," that information can be passed along to unintended audiences. Privacy concerns are also a huge issue. Marketers use geolocation technology to target kids with promotions. A child's purchasing habits will be registered and personal data collected. Location-based technology raises several critical questions and concerns:

- Should mobile geolocation data, persistent IP addresses, and other identifying information be protected for children under age 13—in the same way that name, age, gender, and address information are protected today?
- Do teens understand how their personally identifying information will be used, and do they need additional protections?
- Will this identifying information be used to target kids and teens with new behavioral advertising and marketing campaigns?

Balancing the Good and Bad

Mobile phones and devices can bring new educational and creative opportunities for children. They can also bring increased distractions, and decreased privacy. But whether their impact is positive or negative, mobile phones and portable digital devices are not going away. As parents, teachers, industry leaders, and policymakers we must take steps to ensure that kids can access the benefits of mobile technology and digital media, while protecting them from potential negative consequences.

What Parents Can Do

- Think carefully about whether—and when—your kids need mobile phones and devices, and what phone capabilities, like cameras and texting, are appropriate for their age. Make sure your kids know your rules about when, how, and how often to use them.
- Know the new ways that kids use mobile phones, including creating, accessing, and distributing video, and downloading apps and games. If you don't know what they're doing, you won't be able to set the rules.
- Talk with your kids about privacy and the ways that mobile phones and location-based services can give out their personal information.

---

[22] *http://www.nhtsa.dot.gov/staticfiles/DOT/NHTSA/NRD/Multimedia/PDFs/Human%20Factors/Reducing%20Unsafe%20behaviors/811216.pdf.*

[23] *http://pewinternet.org/Reports/2009/Teens-and-Distracted-Driving.aspx.*

[24] *http://www.commonsensemedia.org/cheating-goes-hi-tech.*

What Educators Can Do

- Teach Digital Literacy and Citizenship in K–12 schools, so that all kids learn how to use digital—and mobile—devices in smart, effective, and responsible ways.[25]
- Establish clear rules about when, where, and how students can—and cannot—use mobile phones and devices at school, and encourage dialogue about why mobile use needs to be limited and responsible.
- Encourage innovative approaches to using mobile devices to expand positive opportunities for learning, creativity, and communication.

What Industry Can Do

- Take increased responsibility for the programs and apps they distribute.
- Use the same tech innovations that let kids access programs and platforms to enable parents to access tools that help them manage their kids' use of mobile devices.
- Develop better parent controls for mobile devices, and make them easier for parents to understand and use.
- Enable parents to access independent ratings and parent advice through mobile devices—for mobile apps and all the other services that kids can now access.

What Policymakers Can Do

- Build digital literacy and citizenship programs in schools and communities, including professional development for educators, and a new Digital Literacy Corps.
- Update the Children's Internet Protection Act (CIPA) and other legislation to reduce barriers to students using personal mobile devices on school networks, so that schools can decide how to set rules that encourage learning in school, at home, and in between.
- Outlaw texting while driving by all drivers and any use of cell phones by teen drivers.
- Update the Children's Online Privacy and Protection Act (COPPA) to address mobile technology and ensure that children's privacy is protected on all media platforms.

Mobile phones and devices are becoming mini-computers that enable kids to access every portal and platform of the digital world—from home, school, or any place in between. Mobile devices and digital media are changing the ways that kids live and learn—and the changes can create opportunities and pose potential dangers.

Kids today are growing up in a mobile, digital world, and we need to give them the digital literacy skills and judgment to access the benefits—and avoid the dangers—of this world. smart phones will change kids' lives. we all share a responsibility for making sure the changes are positive.

Who We Are

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

More than 1.3 million people visit the Common Sense website every month for age-appropriate media reviews and parenting advice. Tens of millions more access our advice and information through our distribution partnerships with leading companies like Comcast, DirecTV, Time Warner Cable, Cox Communications, Facebook, Yahoo, Google, Apple, Disney, Netflix, Barnes & Noble, Best Buy, and others.

Common Sense Media Board of Directors

Rich Barton, Chairman and CEO, Zillow.com
Marcy Carsey, Founding Partner, Carsey-Werner Productions
Chelsea Clinton, Columbia University
James Coulter, Founding Partner, TPG
Geoffrey Cowan, University Professor, The Annenberg School for Communication at USC
April Delaney, President, Delaney Family Fund
John H.N. Fisher, Managing Director, Draper Fisher Jurvetson

[25] For more information, see the Common Sense Media Digital Literacy and Citizenship Whitepaper at *http://www.commonsensemedia.org/about-us/public-leadership*.

Lycia Carmody Fried, Community Volunteer
Thomas J. Holland, Partner, Bain & Company, Inc.
Gary E. Knell, President and CEO, Sesame Workshop
Robert L. Miller, President and CEO, Miller Publishing Group
William S. Price, III (Chair), President, Classic Wines, LLC
Jesse Rogers, Managing Director, Golden Gate Capital
Susan F. Sachs, Partner, Establishment Capital Partners
James P. Steyer, Founder and CEO, Common Sense Media
Gene Sykes, Managing Director, Goldman, Sachs & Co.
Todor Tashev, Director, Omidyar Network
Deborah Taylor Tate, Former FCC Commissioner
Michael Tollin, Founding Partner, Tollin Productions
Eugene Washington, MD, Dean, UCLA Medical School
Lawrence Wilkinson (Vice Chair), Co-Founder, Oxygen Media and Global Business Network

Board of Advisors

Aileen Adams, Chair, The Women's Foundation of California
Larry Baer, Chief Operating Officer, San Francisco Giants
Richard Beattie, Chairman, Simpson Thacher & Bartlett LLP
Angela Glover Blackwell, Founder and CEO, PolicyLink
Geoffrey Canada, Founder and President, Harlem Children's Zone
Ramon Cortines, Superintendent, Los Angeles Unified School District
Yogen Dalal, Managing Director, The Mayfield Fund
Steve Denning, Founding Partner, General Atlantic Partners
Susan Ford Dorsey, President, Sand Hill Foundation
Millard Drexler, Chairman and CEO, J. Crew
Ezekiel Emanuel, MD, PhD; Chair, Department of Clinical Bioethics, The National Institutes of Health
Robert Fisher, Director, GAP Inc.
Arjun Gupta, Founder & Managing Partner of TeleSoft Partners
F. Warren Hellman, Founding Partner, Hellman & Friedman
James Herbert II, President and CEO, First Republic Bank
David Hornik, Partner, August Capital
Omar Khan, President, Insight Strategy & Logic (ISL), Web Site Design
David Lawrence Jr., President, The Early Childhood Initiative Foundation
Nion McEvoy, Chairman and CEO, Chronicle Books
Nell Minow, Founder, The Corporate Library and Movie Mom
Newton Minow, Counsel, Sidley, Austin and Brown; Former FCC Chairman
James Montoya, Senior Vice President, The College Board
Becky Morgan, President, Morgan Family Foundation
Nancy Peretsman, Managing Director, Allen & Company Inc.
Philip Pizzo, MD, Dean, Stanford University School of Medicine
George Roberts, Founding Partner, Kohlberg Kravis Roberts & Co.
Carrie Schwab Pomerantz, President, Charles Schwab Foundation
Alan Schwartz, CEO, Guggenheim Partners
Marshall Smith, Senior Adviser, Department of Education
Thomas Steyer, Founding Partner, Farallon Capital
Robert S. Townsend, Partner, Morrison & Foerster LLP
Laura Walker, President, WNYC Radio
Alice Waters, Founder, Chez Panisse and Chez Panisse Foundation
Robert Wehling, Founder, Family Friendly Programming Forum; Former CMO, Procter & Gamble
Tim Zagat, Co-Founder and Co-Chair, Zagat Survey

Board of Policy Advisors

Angela Glover Blackwell, Founder and CEO, PolicyLink
Dr. Milton Chen, Executive Director, The George Lucas Educational Foundation
Michael Cohen, CEO, The Michael Cohen Group
Dr. Jeffrey Cole, Director, Center For The Digital Future
Ramon Cortines, Superintendent, Los Angeles Unified School District
Ezekiel Emanuel, MD, PhD; Chair, Department of Clinical Bioethics, The National Institutes of Health
Ellen Galinsky, Co-Founder and President, Families and Work Institute
Andrew Greenberg, President, Greenberg Qualitative Research, Inc.
Denis Hayes, President, The Bullitt Foundation
Dr. Donald Kennedy, President Emeritus, Stanford University; Editor-in-Chief, Science Magazine

David Lawrence Jr., President, The Early Childhood Initiative Foundation
Wendy Lazarus, Co-Founder and Co-Director, The Children's Partnership
Christopher Lehane, Political Communications Expert
Laurie Lipper, Co-Founder and Co-Director, The Children's Partnership
Philip Pizzo, MD, Dean, Stanford University School of Medicine
Dr. Alvin Poussaint, Prof. of Psychiatry, Harvard Medical School; Dir. of Media, Judge Baker Children's Center
Thomas Robinson, MD, Associate Professor of Pediatrics and Medicine, Stanford University
Theodore Shaw, Professor, Columbia University
Marshall Smith, Senior Adviser, Department of Education

○