



December 23, 2011

VIA ELECTRONIC DELIVERY

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-113 (Annex E)
600 Pennsylvania Avenue NW
Washington, DC 20580

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

Dear Secretary Clark:

Facebook appreciates the opportunity to comment on the Federal Trade Commission's proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule" or "the Rule"). Facebook commends the Commission for carefully considering the feedback that Facebook and almost seventy other commenters submitted last year in response to the Commission's initial request for comments. The Commission's thoughtful review process has helped produce a proposed COPPA Rule that attempts to balance the goals of protecting children's privacy and safety online and ensuring that innovation in interactive online environments is not unnecessarily stifled.

I. EXECUTIVE SUMMARY

Facebook started in 2004 as a social networking site for college and university students. Over time, our users grew to include teens and adults. Our policies prohibit children under the age of 13 from joining Facebook, and we take our responsibility to protect the privacy and safety of young people seriously. We design our products and services to include robust privacy controls and safety settings, and we couple these protections with comprehensive educational resources to create one of the safest environments on the Internet. We hope that our experience in protecting teens' privacy and safety online can help inform the Commission's efforts to ensure that children's personal information is afforded similar protections.

In enacting COPPA, Congress sought to promote children's privacy and safety on the Internet while ensuring the availability of content for children online.¹ As described in these comments, Facebook fully supports these goals.

¹ See Statement of Sen. Bryan, 144 Cong. Rec. at S11657 (Oct. 7, 1998) (noting that Congress sought "to enhance parental involvement in a child's online activities" to protect children's privacy and safety online "in a manner that

These comments begin by describing some of the many ways in which Facebook safeguards the privacy and safety of minors online. Our comments then turn to the areas where we believe the Commission's proposed changes appropriately implement Congress's aims. For example, we support the Commission's decision to preserve the current age threshold, to retain the actual knowledge standard, and to incorporate new parental consent mechanisms into the COPPA Rule. Our comments conclude with a discussion of other measures that would help clarify the proposed changes and further advance COPPA's goals. Specifically, the Commission should:

- Refine the circumstances under which persistent identifiers will be covered under the COPPA Rule to ensure that operators of child-directed websites and services are not precluded from using social media plugins;
- Streamline the review process for new parental consent mechanisms in a way that will promote innovation and transparency online; and
- Clarify that the third-party data security requirements only apply to businesses with which the operator has a contractual relationship.

These additional steps not only would ensure that parents are empowered to exercise appropriate control over their children's online activities, but also would spark the development of rich, interactive experiences for children online.

II. Facebook Is Committed to Protecting Young People Online.

Nothing is more important to Facebook than keeping people safe. We recognize that special privacy and safety controls are needed to protect young people, and we are committed to preventing the exploitation of youths online. To this end, we have developed a comprehensive approach for promoting the safety and privacy of minors on the Internet.

For example, people who sign up for a Facebook account are required to type in their age on the very first screen. When a person enters a birth date that indicates his or her age is younger than 13, our age gate technology blocks the registration and places a persistent cookie on the device used to establish the account. This persistent cookie helps prevent the child from attempting to circumvent the age screen by back buttoning and providing a different birth date.

We recognize, of course, that the age gate does not always prevent children from registering. Facebook's protections go above and beyond COPPA's requirements and the Commission's recommended best practices by applying a tiered approach to enforcement that combines technical checks at signup, social verifications, and reports from our community to help identify child accounts. We ask people to notify us if they believe we might have received information from a child under 13; we have a dedicated compliance channel for these reports; and we delete the accounts of children under 13 as soon as we become aware of them.

One of Facebook's most important safeguards is our promotion of a real name culture online. We always have believed that people online are more likely to adhere to community rules and less likely

preserves the interactivity of children's experience on the Internet and preserves children's access to information in this rich and valuable medium").

to engage in negative, dangerous, or criminal behavior when their real-world friends and families surround them. A culture of authentic identity also makes our service less attractive to predators and other bad actors who rarely use their real names and email addresses when engaging in nefarious activity. To protect this real name culture, creating an account using a fake name is a violation of our policies and is grounds for closing an account; we have tools to detect fake accounts; and we block the registration of accounts under common fake names.

We also leverage the collective experience of the more than 800 million people on Facebook to keep an eye out for offensive or potentially dangerous content. We make it easy to report offensive or harassing content with “report” links on nearly every page on Facebook, and we have systems to prioritize the most serious reports. A trained team of reviewers responds to reports and escalates them to law enforcement as needed.

We offer a number of additional tools to ensure that individuals have a positive experience when using our site, including:

- Inline privacy settings. According to a recent Yahoo! study, 81 percent of teens use privacy controls when setting up an online profile.² Facebook now also offers inline privacy settings, meaning that the settings can be adjusted at the point where the user decides to share a particular piece of information. We made the icons for each of the different privacy settings prominent and easy to identify, so that users can easily understand whom they are sharing with at that moment. An example of these inline privacy settings is included in Appendix A.
- Age-appropriate sharing and visibility settings. Facebook’s privacy and visibility settings take into account the unique needs of people between the ages of 13 and 17, and are more restrictive than the settings for adults in nearly all cases. For example, a minor’s sharing is automatically restricted to no more than the minor’s friends and friends of those friends, or their networks, which are typically associated with their schools.³ Minors never have listings created for them in search engines off of Facebook, and the ability to share their location is automatically defaulted to “off.” Unlike adults, minors can only be “tagged” on Facebook by their friends or the friends of those friends. Facebook’s “Tag Review” feature, which is a privacy option that allows people to approve or reject tags that others add to their posts, is automatically turned “on” for minors.
- Safeguards to avoid inappropriate contact between adults and minors. Facebook employs robust tools to protect minors from unwanted contact and solicitation. For example, minors can only receive Messages on Facebook from friends or the friends of those friends, and never by strangers. Additionally, when a minor who is new to our service receives a friend request, we might interpose a message along the lines of “Only accept friend requests from people you really know” before the minor can confirm that he or she wants to accept the friend request. We also use innovative technical mechanisms to flag suspicious adult behavior. For instance, if an adult sends an unusual number of friend requests to minors

² See Yahoo! Strategic Insights & Research, *Yahoo! 2011 Online Safety Survey* (Oct. 2011), http://epsolution.zenfs.com/wpprod/14/2011/10/Yahoo-2011-Online-Safety-Report_short-version.pdf.

³ The label for this sharing may be “Public” but for minors this has been defined to include only “Friends” and “Friends of Friends.”

that are ignored or rejected, our warning systems might be triggered, which initiates a Facebook inquiry so that remedial action can be taken, if necessary.

- Ongoing authentication checks. We perform technical and community verification of users' accounts. Although we do not generally discuss the details publicly in order to limit attempts to compromise or circumvent the safeguards, we look for anomalous behavior in the aggregate data produced by the Facebook community and employ automated systems to block inappropriate conduct, warn the user, or, when necessary, disable the offending account.
- Social Reporting. Facebook believes in offering teens many options to manage their reputations, and to seek help should they ever encounter abuse on the site. A new tool we have pioneered called "Social Reporting" allows minors to directly notify others of content they want removed from Facebook, such as an unflattering or embarrassing photo posted by a friend. In cases where teens may feel threatened by posted content, the Social Reporting feature gives them the option to report the content to Facebook, to send a copy of the content to a trusted adult, or to block the person who posted it. Appendix B illustrates the many choices that users have when they encounter harassing or abusive content. By giving teens more options to address unwanted behavior, we have allowed them to resolve issues more efficiently than was previously possible.
- Blocking registered sex offenders. We work proactively to identify and prohibit access by registered sex offenders. We also have been involved in efforts to establish a national database of registered sex offenders that enables real-time checks and includes important electronic information like email addresses and IM handles.
- Preventing child exploitation. We have a zero tolerance policy regarding child exploitative material on our platform and employ innovative and industry-leading measures to prevent its dissemination. We build complex technical systems that either block the creation of this content, including in private groups, or flag it for immediate review by our safety team. In collaboration with Microsoft and the National Center for Missing and Exploited Children ("NCMEC"), we also utilize a technology called PhotoDNA to scan every photo uploaded to Facebook. PhotoDNA allows us to instantaneously identify, remove and report known abusive images to NCMEC, which coordinates with law enforcement authorities around the world for potential prosecution. PhotoDNA is a game-changing technology that has helped ensure an online experience that is free from these abusive materials.
- Amber Alerts. Earlier this year, Facebook teamed with NCMEC and law enforcement to use our platform to widely and rapidly distribute Amber Alerts, the potentially life-saving bulletins that a child has been abducted or gone missing, to communities across the United States. We created 53 AMBER Alert Facebook Pages, one for each U.S. state and territory, and residents who "Like" their state's AMBER Alert Facebook Page automatically receive notifications in their News Feed when an Amber Alert is activated for a child in that state. These users also can share that information with Friends, which creates a viral means of immediately spreading the word that a child needs help, especially in those crucial first hours after an abduction.

In addition to these tools, we have taken additional measures to enhance the privacy and safety of our teen users:

- Encouraging parent-child conversations. Communication between parents, teachers, and children about safe use of the Internet is vital. Just as parents must teach their children how to cross the road safely, parents must recognize that they should talk to their children about safe online practices. A recent study from the Pew Research Center found that 93 percent of parents of online teenagers have talked with their children about ways to use the Internet and cell phones safely.⁴ Our Family Safety Center provides detailed and helpful advice to help support parents and teachers in these conversations.⁵
- Combating bullying and online harassment. Our Statement of Rights and Responsibilities,⁶ the governing document for our site, prohibits the posting of content that bullies or harasses. As explained above, we empower users to serve as “community policemen” in reporting offensive content, and our dedicated team of professionals reviews, prioritizes, and acts upon these reports. We also provide educational materials through our Family Safety Center and blog that specifically address bullying prevention, and we have partnered with other organizations to educate young people about the responsibilities of digital citizenship and the dangers of abuse online. For example, we are currently promoting the Stop Bullying: Speak Up campaign with Time Warner. We have mobilized tens of thousands of people to stand up to bullying on Facebook’s own site, and have bolstered that message via Time Warner properties like CNN, Cartoon Network, and Sports Illustrated.⁷
- Facebook Safety Page. Over 680,000 people have “Liked” our Safety Page,⁸ which allows them to receive the latest in safety education directly in their Facebook News Feeds. We regularly post information, tips, articles, features, and dialogues about digital citizenship, as well as links to useful content from third-party experts.
- Digital Citizenship Research Grants. Our new Digital Citizenship Research Grants program is an effort to support world-class research that improves understanding of the challenges and opportunities associated with how teens are growing up in a world of digital media and technology. As part of this initiative, Facebook is investing \$200,000 to support research

⁴ Pew Research Center, *Teens, Kindness and Cruelty on Social Network Sites* 67-68 (Nov. 9, 2011), <http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>.

⁵ Facebook, Family Safety Center, <http://www.facebook.com/safety> (last visited Nov. 17, 2011).

⁶ Facebook, Statement of Rights and Responsibilities, <http://www.facebook.com/legal/terms> (last visited Dec. 17, 2011).

⁷ See, e.g., Facebook, Stop Bullying: Speak Up, <http://www.facebook.com/stopbullyingspeakup> (last visited Nov. 17, 2011); CNN, Stop Bullying: Speak Up, <http://www.cnn.com/SPECIALS/2011/bullying/> (last visited Nov. 17, 2011); Cartoon Network, Stop Bullying: Speak Up, <http://www.cartoonnetwork.com/promos/stopbullying/index.html> (last visited Nov. 17, 2011); Michael Rosenberg, *Time to Stand Up*, Sports Illustrated, Oct. 10, 2011, <http://sportsillustrated.cnn.com/vault/article/magazine/MAG1191014/index.htm>.

⁸ Facebook, Facebook Safety, www.facebook.com/fbsafety (last visited Nov. 17, 2011).

that highlights trends associated with digital citizenship, with an initial focus on bullying prevention. This research program has been open to academic and nonprofit institutions.

- Community outreach. Facebook regularly engages directly with parents, teachers, and teens around the country. We have developed a program to do live safety demonstrations for these audiences, as well as members of government, on a regular basis in both English and Spanish.
- Involvement in online privacy and safety initiatives. We believe online safety is a shared responsibility, which is why we partner with organizations globally to create the most robust and effective safety environment possible. We have proactively convened a global Safety Advisory Board, comprised of five leading experts in family safety (Childnet International, ConnectSafely.org, the Family Online Safety Institute, the National Network to End Domestic Violence, and WiredSafety), who advise us on best practices. We are also proud of our work with government officials and other experts—including the U.S. State Attorneys General, the Internet Safety Technical Task Force, the EU Safer Internet initiative, the National Suicide Prevention Lifeline, and the National Cyber Security Alliance, as well as many others—to promote safety and privacy online.

Many of the tools we have adopted and measures we have taken are unprecedented in the industry, and we believe that these safety, security, and privacy efforts advance the cause of online safety for minors.

III. In Key Areas, the Proposed Rule Advances COPPA’s Goals of Empowering Parents and Creating Incentives for Child Privacy and Safety Innovation Online.

The Internet has undergone revolutionary changes in the thirteen years since COPPA was enacted. Even back in 1998, however, Congress had the foresight to recognize that the “Internet offers unlimited potential for assisting our child[ren]’s growth and development.”⁹ Congress thus sought to “enhance parental involvement in a child’s online activities” to protect children’s privacy and safety, and to do so in a way that would “preserve[] the interactivity of children’s experience on the Internet and . . . children’s access to information in this rich and valuable medium.”¹⁰ Three of the recommendations in the Commission’s proposed rulemaking respect and promote these goals.

A. The under-13 age threshold strikes an appropriate balance between promoting parental engagement and respecting teens’ privacy and constitutional rights.

We support the Commission’s recommendation that COPPA not be expanded to cover teens. Facebook agrees with the Commission’s observation that increasing the age threshold could impair adolescents’ constitutionally protected right to access information and express themselves. There is no question that the First Amendment also protects teens.¹¹

⁹ Statement of Sen. Bryan, 144 Cong. Rec. at S8483 (July 17, 1998).

¹⁰ *Id.*

¹¹ See, e.g., *Erznoznik v. Jacksonville*, 422 U.S. 205, 212–13 (1975) (“[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar

The Commission also correctly notes that “COPPA’s parental notice and consent approach is not designed to address” the particular privacy challenges that teens face online.¹² In addition to the practical challenges noted by the Commission, requiring operators to give parents access to, and the ability to delete, their teens’ online accounts could be counterproductive in many situations. Where the parent/child relationship is not a positive one—for instance, where a teen is suffering abuse at the hand of a parent—some teens may choose to reach out electronically to teachers, counselors, or trusted friends for guidance. Parental access in such circumstances could actually impede the teens’ efforts to seek help.

There are more effective and appropriate methods for ensuring that teens understand and can control how their information is used and shared on the Internet. As noted above, Facebook has taken numerous measures—including context-sensitive sharing limitations, restrictions on adults’ ability to share and connect with minors, and ongoing authentication checks—to ensure that minors can communicate with other users in safe and age-appropriate ways. In addition, research shows that most teens are taking advantage of existing tools to help protect themselves online, such as actively managing the circumstances under which they disclose personal information. The Pew Research Center recently found that, among teens who have a social media profile, 62 percent use private profiles so that only their friends can see the content they post.¹³

- B. The Commission is correct to retain the “actual knowledge” standard, which promotes innovation in online privacy and safety protections.

The Commission rightly proposes to retain the actual knowledge standard for operators of general-audience websites and online services. As the Commission correctly observes, imposition of a “reasonable efforts” or “constructive knowledge” standard would be far less workable and unduly burdensome for operators. Requiring operators of general-audience websites and online services to “ferret through a host of circumstantial information to determine who may or may not be a child,”¹⁴ including potentially millions of user posts and profiles, would be a herculean task with minimal benefit because, in many cases, this circumstantial evidence would be inconclusive.

As discussed above, Facebook has implemented sophisticated algorithms and social engineering tools that combine social verifications, community reporting, ongoing authentication checks, and other technical measures to help prevent underage children from using our service. These efforts go well beyond what is required by COPPA and industry best practices.

Despite these industry-leading efforts, a number of children, sometimes with the assistance of their parents, reportedly have been able to sign up on social networking services.¹⁵ In particular, a group of researchers has found that some parents know that their children joined Facebook when they

public dissemination of protected materials to them.” (citation omitted)); *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969) (recognizing that teenagers have a right to express their opinions at school).

¹² Children’s Online Privacy Protection Rule, 76 Fed. Reg. 59,804–05 (Sept. 27, 2011).

¹³ Pew Research Center, *supra* note 4, at 60.

¹⁴ Children’s Online Privacy Protection Rule, 76 Fed. Reg. at 59,806.

¹⁵ As discussed above, when Facebook becomes aware of accounts established by children under the age of 13, we terminate those accounts.

were younger than what the parents believed to be the minimum age requirement for use of the site. Indeed, among the parents who know that their child joined Facebook while under the age of 13, 68 percent of the parents helped the child create the account.¹⁶ These findings demonstrate why adopting a “constructive knowledge” standard would be unworkable. In a world where parents actively assist their children to circumvent age restrictions, operators of general audience websites and online services cannot be held to a “constructive knowledge” standard. This standard would subject operators to expectations that they simply could not meet.

Amending the COPPA statute to impose a “constructive knowledge” or similar standard also could have unintended consequences that undermine the goals of the statute. For instance, requiring operators of general-audience sites and online services to take additional steps to investigate or verify the ages of their users in some cases could result in the *increased* collection of data from and about children—with all the attendant privacy and safety risks. Moreover, because no preventative measures are foolproof, a “constructive knowledge” standard would create legal uncertainty that would make it far riskier for website operators and service providers to experiment with privacy and safety enhancing technologies, thereby discouraging innovation in these areas. To avoid these unintended consequences, the “actual knowledge” standard should be retained as proposed in the amended COPPA Rule.

C. The Commission’s recognition of new parental consent mechanisms appropriately reflects changes in technology.

In our earlier comments to the Commission, we urged the Commission to use the COPPA Rule review process to facilitate the introduction and approval of new mechanisms for acquiring verifiable parental consent. We are encouraged that the Commission has chosen to do so, and we commend the Commission for promoting the development of new ways to obtain parental consent.

New ways of obtaining parental consent are needed because some of the existing consent mechanisms require the use of technology or devices that parents may not have. If a child’s parent does not have a credit card, for example, the child will be precluded from using any sites or services that rely on the credit card method for obtaining parental consent. Similarly, because not every parent has a printer or fax machine at home, the written consent method could present difficulties for some parents. It is therefore important that operators have a broad menu of options for seeking parental consent, including web-based mechanisms, so that even parents who lack access to certain offline resources can still ensure that their children have rich and meaningful experiences online.

Facebook agrees with the Commission that the three additional mechanisms recognized in the proposed Rule meet the statutory standard of being a “reasonable effort (taking into consideration available technology) . . . to ensure that a parent of a child receives notice of the operator’s personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.”¹⁷

¹⁶ See, e.g., Danah Boyd et al., “Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the ‘Children’s Online Privacy Protection Act,’” First Mon. (Nov. 7, 2011), <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075>.

¹⁷ 15 U.S.C. § 6501(9).

- Scanned versions of signed consent forms. A consent form that is electronically scanned and transmitted to the operator is functionally no different from a form that is returned by postal mail or facsimile—both of which are well-accepted means of securing parental consent. Scanning technology was still in its infancy when the COPPA Rule was initially promulgated, but today many parents have ready access to scanners. By recognizing that scanned versions of signed consent forms constitute a reasonable means of obtaining parental consent, the Commission is appropriately updating the Rule to account for changes in technology.
- Video verifications. Videoconferencing, like scanning, is a technology that has become much more common since the COPPA Rule was promulgated in 2000. It is in some ways an even more reliable way of ensuring that the person providing consent is the child’s parent than the long-established telephone consent method, because it allows both visual and aural confirmation of a parent’s identity.
- Verification using a parent’s government-issued identification. In part because the Commission already endorsed this method through its approval of the Privo safe harbor application in 2004, our understanding is that a number of companies currently rely on this method.¹⁸ The Commission’s position is just as strong today as it was back in 2004; using available technology to check the driver’s license number or a portion of a Social Security number provided by the parent against existing databases of government-issued identifiers reasonably ensures that the person providing consent is the child’s parent. This approach achieves the delicate balance of making it easy for the parent to provide consent, while making it difficult for the child to pose as the parent. In addition, when combined with responsible data disposal practices, this method also protects the parent’s information against unauthorized use or disclosure.

As the Commission continues its consideration of these and other parental consent mechanisms, it is important to keep Congress’s original directive in mind: parental consent should “tak[e] into consideration available technology.”¹⁹ The Internet has evolved away from the old model of static, bilateral relationships where the user interacted with one service provider at a time. Today, the online experience frequently involves multiple companies offering various applications, video services, games, and other features through a single online interface or platform.

In these “multiple operator” scenarios, it is becoming increasingly unworkable for each of the operators to provide notice and obtain parental consent. For example, the Commission’s proposed elimination of the multiple operator exception would require that the online notice state not only the contact information for each operator that collects or maintains personal information through the site or service, but also “a description of what information each operator collects from children, . . . how such operator uses such information, and; the operator’s disclosure practices for such information.” As the Internet continues to move toward joint services scenarios, these kinds of detailed recitations are likely to become increasingly overinclusive and overwhelming. A single child likely will only install, use,

¹⁸ See Letter from C. Landis Plummer, Acting Secretary, Fed. Trade Comm’n, to Albert Strong, Director, Privacy Assurance Program, Privo, Inc. (July 29, 2004), <http://www.ftc.gov/os/2004/08/040802privoletter.pdf>; Privo Safe Harbor Application, at 24–26 (Mar. 3, 2004), <http://www.ftc.gov/os/2004/04/privoapp.pdf>.

¹⁹ 15 U.S.C. § 6501(9) (defining “verifiable parental consent”).

or play a handful of the applications, video services, games, or other online features offered through the integrated online interface or platform. The proposed Rule, however, could be interpreted to require operators to provide parents information about the contact details and data-handling practices of every operator active on the platform, regardless of whether that particular operator actually interacts with the parent's child. The Commission's proposal therefore could wrongly cause parents to believe that more entities collect personal information from the parent's child than actually do; make it difficult for a parent to determine who should be contacted to answer the parent's questions; and hamper the parent's ability to make informed decisions, thereby undermining COPPA's goal of empowering parents.

Because the future of the Internet will increasingly involve multiple operators working together to offer seamless online experiences, future notice and parental consent mechanisms should be designed to facilitate these kinds of integrated, interactive services. Specifically, the Commission should confirm that one operator can provide notice and obtain consent on behalf of other individual operators, provided that parents have control over all operators' use of their child's information consistent with COPPA's goal of enhancing parents ability to understand, control and supervise their child's online activities.

IV. There Are Additional Steps the Commission Could Take to Enhance Parental Involvement and Spark Development of Rich Content and Innovative Online Privacy and Safety Protections.

When COPPA was first enacted in 1998, Congress was well aware that technology and user expectations would continue to evolve.²⁰ And, although the Commission typically reviews its rules every ten years, the Commission undertook this latest review of the COPPA Rule only five years after completing its last update because of the "rapid-fire pace of technological change" in how children are accessing and using Internet-enabled technologies.²¹

Regardless of whether the next COPPA Rule review occurs five or ten years from now, the Commission must ensure that the requirements it puts in place today provide sufficient flexibility to accommodate the technological revolutions that will take place in the years to come. Five years, much less ten years, is an eternity by Internet standards. Five years ago, Facebook was a distant third in the competition to become the most popular social networking service in the United States; the leading site, MySpace, had more than three times as many monthly visitors.²² The only thing that is certain is that there is no way to predict what new technologies and services will emerge over the next decade.

In order to foster private-sector efforts to increase parental involvement and create rich, interactive experiences for children online, there are three additional steps that the Commission should take to amend its proposed COPPA Rule.

²⁰ 15 U.S.C. § 6501(9); *see also* Statement of Sen. Bryan, 144 Cong. Rec. at S11657 (Oct. 7, 1998) (directing the FTC to interpret the requirements for notice and consent "flexibly, . . . 'taking into consideration available technology'").

²¹ Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59,804.

²² comScore, Press Release, "Social Networking Sites Continue to Attract Record Numbers as Myspace.Com Surpasses 50 Million U.S. Visitors in May" (June 15, 2006), [http://www.comscore.com/Press Events/Press Releases/2006/06/MySpace Surpasses 50 Million Visitors](http://www.comscore.com/Press%20Events/Press%20Releases/2006/06/MySpace_Surpasses_50_Million_Visitors).

A. The Commission should clarify how persistent identifiers will be treated under the COPPA Rule to promote interactive, social experiences for teens online.

A number of websites and online applications currently rely on social media “plugins” to facilitate the communication of ideas and content online. These social media plugins can help enrich users’ social, cultural, and educational experiences in many innovative ways. For instance, some businesses are using web-based learning communities to support new levels of social exchange and interaction that, in turn, promote and foster student motivation and educational development. Some examples include applications on Facebook such as “weRead,” which enables people to find and review books and get book recommendations from their friends, or “Flashcard Exchange,” which allows students to browse for or create flashcard sets on any subject and use study tools to aid with memorization. Other Facebook applications like “Causes” provide an online platform for individuals and organizations to raise funds for charitable causes.

Operators of websites and applications that arguably are directed to children sometimes include social media plugins on their sites or online services to reach teens and parents who also may visit or use their products and services. For example, a website or application that is attractive to users between the ages of 9 and 14 may be deemed to be “directed to children” if the site or service features models under the age of 13, childish language, kid-friendly music, animated characters, and child-oriented activities and incentives, even though a sizable number of its users may be 13 years old or older.²³

We urge the Commission to clarify that operators may include social media plugins on child-oriented websites without triggering COPPA’s requirements.

1. *Background on Facebook’s social plugins.*

Facebook offers a number of social plugin tools, including the Facebook “Like” and “Recommend” buttons that developers may integrate into their websites and online applications using a line of HTML code.²⁴ Importantly, Facebook specifically designed its social plugins so as not to share information that people provide on Facebook with third-party sites. To do this, the social plugin pulls content directly from Facebook’s website and sends it to the person’s browser, allowing, in effect, a part of Facebook to appear on a non-Facebook site.

When a person who has never visited Facebook.com before visits a website with a social plugin, Facebook will receive and record through social plugins a limited list of standard browser information, including: (i) the website being visited, (ii) the date and time, (iii) the IP address of the computer, and (iv) information about the browser type and operating system. The transmission of this information is part of the normal operation of the Internet: the information is sent to Facebook so that its servers can communicate with the person’s browser and load the Facebook functionality onto the webpage.

In addition to this technical information, if the person has visited Facebook.com in the past, Facebook will record information that has been stored in a “cookie” that was previously set when the person visited our site. For people who have visited Facebook.com using their browser, we place a cookie on their browser that identifies the individual browser but does not include personally identifying

²³ See 16 C.F.R. § 312.2.

²⁴ Facebook, Social Plugins, <http://developers.facebook.com/docs/plugins/> (last visited December 20, 2011).

information, such as name or contact information. This browser-identifying cookie helps us keep Facebook and the people who use it safe. For example, we want to know if the same browser is attempting to visit Facebook thousands of times in just a few seconds as part of a coordinated denial of service attack. Cookies help us prevent such attacks, and the more coverage of browsers visiting Facebook, the more effective this security feature is at protecting the people that use Facebook.

When a person is logged into Facebook and then visits a third-party site with a social plugin, the amount of information we record differs as needed to provide the personalized, social experience that people request when they login to Facebook. Specifically, when a person is logged in to Facebook, we use a cookie to confirm that the person is logged in to a specific Facebook account so that we can customize the content presented through the social plugin with information about a person's friends and ensure that when someone clicks the "Like" button, the "Liked" information is associated with the right account.

Facebook also has agreed to several new policy commitments around the retention of user data. These commitments include amendments to our data retention policy for social plugin impression logs. Specifically, under our revised policy, for people who are not Facebook users or who are Facebook users in a logged out state, Facebook will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, Facebook will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, Facebook will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com.²⁵

2. *The inclusion of social plugins on child-directed sites should not trigger COPPA.*

By expanding the definition of "personal information" to include persistent identifiers, such as IP addresses and cookie IDs, the proposed COPPA Rule creates ambiguity about whether social media plugins can be included on websites and online services that are directed to children absent verifiable parental consent. As explained below, the better reading of the proposed COPPA Rule is that websites may use these social plugins without triggering COPPA's requirements. The Commission could avoid this ambiguity by focusing the definition of "personal information" on those uses of persistent identifiers which cause the Commission concern — namely, online behavioral advertising.²⁶ Alternatively, the Commission could explicitly state that the inclusion of social plugin tools on child-directed sites results in neither a "disclosure" nor a "collection" of children's personal information online for purposes of COPPA.

With respect to users who are logged in or are logged out of Facebook and who visit a child-directed site, COPPA's requirements clearly are not triggered. These users represented to Facebook when they created their Facebook account that they are at least 13 years old. Unless Facebook obtains

²⁵ See Ireland Data Protection Commissioner, *Report of Audit*, at 74 (Dec. 21, 2011), <http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf>. As the Irish Data Protection Commissioner recognizes, from time to time litigation is filed against Facebook that requires the company to retain data for purposes of such litigation, including social plugin data.

²⁶ See Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59,811–12 (noting that "methods of marketing online have burgeoned in recent years" and stating that parental consent will be required where persistent identifiers are used for the purpose of "behaviorally targeting advertising to the child").

actual knowledge that a particular user is under the age of 13, such as where Facebook is contacted by a concerned parent who has discovered his or her child misstated the age information, circumstantial information that a user could be a child because he or she visited a child-directed website does not trigger COPPA.²⁷ In addition, the statute is clear that a “child” is an individual under the age of 13.²⁸ The statute prevents the Commission from restricting the collection or disclosure of personal information from a user who is 13 years old or older, even if such collection or disclosure occurs on websites and applications that are directed to children. The Commission therefore is foreclosed from expansively interpreting COPPA to reach these users.

With respect to individuals who do not have Facebook accounts, inclusion of social media plugins does not result in a “disclosure” to or a “collection” by Facebook for two reasons.

First, Facebook uses the persistent identifiers that it collects for limited purposes that support the internal operations of the social plugin tool that the website operator included on the website. The Commission appropriately recognized “that when a persistent identifier is used only to support the internal operations of a Web site or online service” then “the concerns underlying COPPA’s purpose are not present.”²⁹ Facebook’s social plugin tool records IP address and cookie ID for limited purposes, such as ensuring that the social plugin is working properly. Significantly, this information is not used for online behavioral advertising purposes. Because Facebook’s use of IP address and cookie ID is used “to aid the functionality and technical stability of Web sites and online services and to provide a good user experience,” the Commission clearly “does not intend to limit operators’ ability to collect such information from children.”³⁰ Facebook encourages the Commission to make this point more explicit within the COPPA Rule.

Second, with respect to the IP address, Facebook is taking reasonable measures to render the user’s IP address de-identifiable. The Commission has explained that no collection occurs if personal information is removed from a child’s posts before they are made public in online forums.³¹ Similarly, the Commission has suggested that operators can avoid collecting personal information so long as it is immediately altered or hashed in such a way “that [it] can no longer be reconstructed into [its] original form.”³² The proposed COPPA Rule reinforces these longstanding policies by replacing the “100% deletion standard” with a more relaxed standard; an operator does not “collect” personal information as long as the deletion technologies it uses are “reasonably designed to capture all or virtually all

²⁷ See Fed. Trade Comm’n, *Frequently Asked Questions about the Children’s Online Privacy Protection Rule*, at Question 39, 41(a) (Oct. 7, 2008), <http://www.ftc.gov/privacy/coppafaqs.shtm#teen>; Children’s Online Privacy Protection Rule, 76 Fed. Reg. at 59,806 (refusing to replace the “actual knowledge” standard with a lesser “reasonable efforts” or “constructive knowledge” standard that would “require operators to ferret through a host of circumstantial information to determine who may or may not be a child”).

²⁸ See 16 C.F.R. § 312.2 (defining “collection” as the “gathering of any personal information *from a child*” and “disclosure” as the “release of personal information collected *from a child*” or “[m]aking personal information collected *from a child* by an operator publicly available” (emphasis added)).

²⁹ Children’s Online Privacy Protection Rule, 76 Fed. Reg. at 59,812.

³⁰ *Id.* at 59,809–10.

³¹ Fed. Trade Comm’n, *Frequently Asked Questions about the Children’s Online Privacy Protection Rule*, at Question 41(b) (Oct. 7, 2008), <http://www.ftc.gov/privacy/coppafaqs.shtm#teen>.

³² *Id.* at Question 45.

personal information inputted by children.”³³ As the Commission correctly has recognized, the privacy and safety concerns that COPPA was designed to address are not implicated where children’s personal information is deleted or anonymized. Consistent with this guidance, no “collection” or “disclosure” of IP address occurs through the social plugin tool in those instances where Facebook’s policy is to remove from social plugin impression logs the last octet of the IP address when this information is logged.

For the above reasons, we request that the Commission amend its proposed COPPA Rule to clarify that operators of child-directed sites and online services may include social media plugins without obtaining parental consent. Such an approach would create more legal certainty for operators and facilitate the development of innovative, engaging online content for teens.

B. The process for seeking approval of new parental consent mechanisms should be streamlined.

The Commission, noting that “there appears to be little technical innovation in any area of parental consent,” proposes to establish a new process for companies to seek Commission approval of a particular parental consent mechanism. Facebook understands and appreciates the Commission’s dismay at the lack of innovation in this area, and we share the Commission’s belief that operators should be encouraged to explore technological advancements that promote parental engagement and involvement. We recognize that robust consent experiences are crucial for ensuring that parents can meaningfully supervise their children’s online activities.

The Commission could do even more to foster the development of new parental consent mechanisms if it shortened the proposed 180-day timeline for the review process. In the Internet space, it is not unusual for a product to go from conception to launch in less than six months. Indeed, consumers expect and demand a constant stream of innovative new services as well as iterative improvements in the services they already enjoy using. Given the speed with which technologies, user expectations, and consumer services evolve, innovation is more likely to be hindered than helped by a six-month waiting period. In light of the Commission’s extensive experience with COPPA and online privacy more generally, the Commission already has the expertise to make a determination about a particular parental consent mechanism in a more expedited fashion. In other situations where agencies are asked to provide advisory opinions or approve a course of action, agencies often commit to significantly shorter turnaround times.³⁴

³³ Children’s Online Privacy Protection Rule, 76 Fed. Reg. at 59,808.

³⁴ For example, private parties can request business review letters from the Department of Justice’s Antitrust Division to learn about the Division’s enforcement intentions with respect to proposed business conduct. “[F]or business reviews concerning export trade, a response will be issued within 30 business days from the date that the Division receives all relevant data.” U.S. Dep’t of Justice, Introduction to Antitrust Division Business Reviews, <http://www.justice.gov/atr/public/busreview/276833.pdf> (last visited Nov. 17, 2011). For business reviews involving proposals to form joint ventures or to collect and disseminate business information, “the Department will make its best effort to resolve the business review request within sixty to ninety days.” U.S. Dep’t of Justice, Press Release, Pilot Program Announced to Expedite Business Review Process, Dec. 1, 1992, <http://www.justice.gov/atr/public/busreview/201659a.pdf>. Taxpayers can request a letter ruling from the Internal Revenue Service (“IRS”) to obtain a written determination about the taxpayer’s status for tax purposes or the tax effects of a particular transaction. An IRS representative will contact the taxpayer “within 21 calendar days” after the request has been received in the branch office with jurisdiction over the issue, to discuss (among other things)

We support the Commission’s desire to provide transparency, which is important for ensuring that the public and other operators can stay abreast of ongoing developments in this area. However, releasing the proposed mechanism for public comments before the Commission has issued a decision could negatively affect innovation: it would reduce the economic incentives of operators who wish to use their proprietary consent mechanism as a competitive differentiator. The proposed approval process will force operators to disclose their plans to the public—including rival operators—in advance of actual implementation. Because of the long lead-time built into the proposed approval process, rival operators might be able to copy the mechanism, thus destroying the first innovator’s competitive edge.

A better way of ensuring transparency would be for the Commission to publicly release a letter after it has made its decision that explains why the Commission approved or disapproved the particular mechanism. This kind of public notice would allow the Commission to effectively signal which consent mechanisms appropriately protect children, without unduly slowing down the review process or creating competitive concerns. It is also more consistent with the approach that has been adopted by the Commission and other agencies when issuing advisory opinions, staff interpretations, or similar documents.³⁵

Although the Commission has been careful to emphasize that the new approval process will be entirely voluntary, the availability of an approval process could make operators reluctant to use mechanisms other than those specifically set forth in the Rule or approved by the Commission. To ensure that the approval process does not inadvertently deter innovators from introducing new ways to obtain robust parental consent, the Commission should implement a quicker review process with public notice after the Commission has reached a decision.

C. The third-party data security requirements should be clarified.

We understand that the Commission’s proposed amendment to Section 312.8 of the Commission’s COPPA Rule intends to address the “security issues surrounding business-to-business releases of data.” Consistent with this important goal, we encourage the Commission to clarify two aspects of its proposal.

First, we ask that the Commission clarify that the proposed data security requirements apply only to service providers and third-party businesses with which the operator has a contractual relationship. Requiring operators to monitor the security practices of all third parties could be

the representative’s preliminary recommendation and whether the taxpayer should submit additional information. *See* Rev. Proc. 2011-1, § 8.02. A national bank that wishes to commence fiduciary powers must obtain approval from the Comptroller of the Currency (“OCC”). The application to exercise fiduciary or trust powers is not subject to a public comment period and is deemed approved for certain applicants if the OCC does not take action within 30 days. *See* Comptroller’s Licensing Manual: Fiduciary Powers 5 (June 2002), <http://www.occ.gov/publications/publications-by-type/licensing-manuals/fiduc.pdf>.

³⁵ *See* 16 C.F.R. § 1.4 (“Written advice [from the Commission or staff] rendered pursuant to this section and requests therefore, including names and details, will be placed in the Commission’s public record *immediately after the requesting party has received the advice* . . . ” (emphasis added)). Business review requests submitted to the Department of Justice’s Antitrust Division, and the Division’s letter in response, are placed in a public file “[s]imultaneously upon notifying the requesting party of and Division action” as described in the regulations. 28 C.F.R. § 50.6(10).

impractical in the context of websites or online services that allow users to publicly post content or communicate with other users online. The current definition of “third party” in Section 312.1 sweeps so broadly that it also encompasses other users who can view content or receive communications from the child—including, for example, the child’s relatives or classmates. Under the proposed amendment, operators would be obligated to take reasonable measures to ensure that these relatives and classmates have “reasonable procedures” in place to protect the child’s personal information. The proposed Rule leaves it unclear what these “reasonable procedures” might be.

Second, we ask the Commission to clarify the obligation to “take reasonable measures to ensure” that these third parties appropriately protect children’s personal information. Through its enforcement actions, the Commission has made clear that companies have an obligation to safeguard the data they collect.³⁶ Reasonable data security measures are already standard in the industry, and responsible companies already take strong measures to ensure that they only do business with partners who can adequately protect shared data. As drafted, the proposed data security requirements are so broad that they could create ambiguity about third-party obligations. The Commission clearly did not intend that the word “ensure” requires operators and their service providers to negotiate every contract anew. If the Commission requires companies to implement special protections just for data collected from children under 13, companies might respond by opting not to collect that information at all—which would chill the development of rich Internet experiences for children. Accordingly, the Commission should clarify that the security obligation within the COPPA Rule requires operators to (1) develop and use reasonable steps to select and retain service providers that are capable of appropriately protecting the privacy of the personal information they receive from the operator and (2) require service providers, by contract, to implement and maintain appropriate privacy protections for such personal information.

* * *

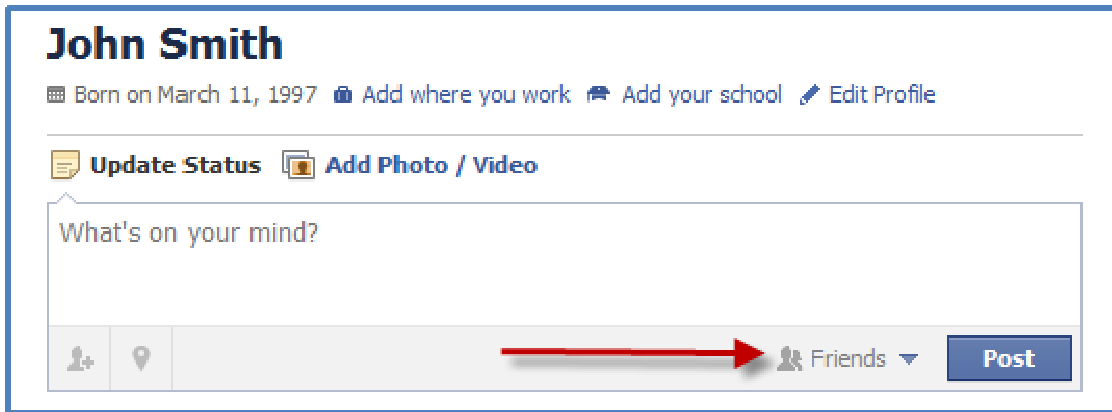
Thank you for the opportunity to comment on the proposed Rule. We applaud the Commission’s thoughtful approach to the COPPA Rule revision process, and we support the Commission’s efforts to modernize the Rule in a way that encourages companies to innovate in their efforts to keep young people of all ages safe online.

Respectfully submitted,

Erin M. Egan
Chief Privacy Officer, Policy
Facebook

³⁶ See also Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, at 45 (Dec. 2010) (“The idea that companies should provide reasonable security for customer and employee data is well-settled.”).

Appendix A: Example of Inline Privacy Settings



John Smith
Born on March 11, 1997 Add where you work Add your school Edit Profile

Update Status Add Photo / Video

What's on your mind?

Friends Post

A red arrow points to the 'Friends' privacy setting in the status update interface.

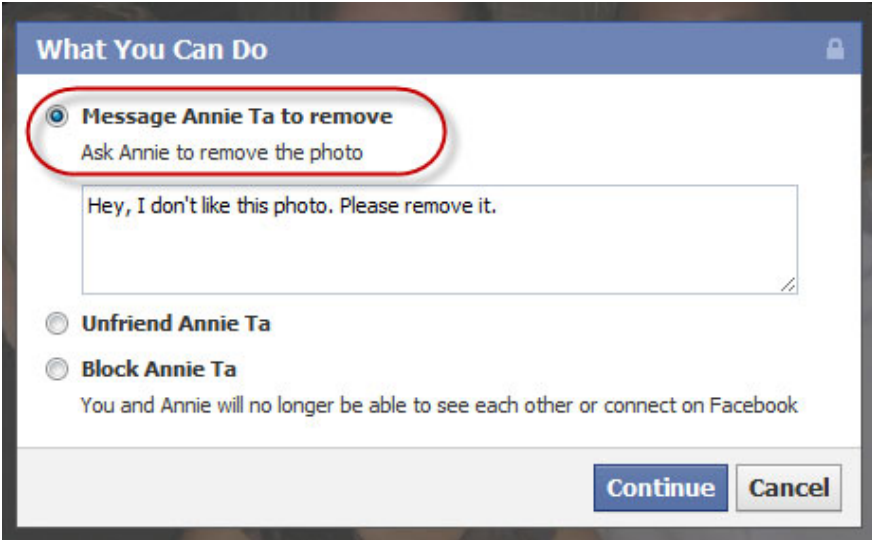
Appendix B: Examples of Social Reporting

1. Users can indicate that they want content to be removed:



The screenshot shows a reporting dialog with a blue header containing the question "Is this photo about you or a friend?" and a lock icon. Below the header, there are two main sections of radio button options. The first section is titled "Yes, this photo is about me or a friend:" and contains three options: "I don't like this photo of me" (which is selected and circled in red), "It's harassing me", and "It's harassing a friend". The second section is titled "No, this photo is about something else:" and contains six options: "Spam or scam", "Nudity or pornography", "Graphic violence", "Hate speech or symbol", "Illegal drug use", and "My friend's account might be compromised or hacked". At the bottom left, there is a link "Is this your intellectual property?". At the bottom right, there are two buttons: "Continue" and "Cancel".

2. Users can send a private message to the person who posted the content they wish to be removed. Because this action takes place in "private," teens are more likely to use it.



The screenshot shows a reporting dialog with a blue header containing the title "What You Can Do" and a lock icon. Below the header, there are three radio button options. The first option, "Message Annie Ta to remove", is selected and circled in red. Below this option is a text input field containing the message "Hey, I don't like this photo. Please remove it." The second option is "Unfriend Annie Ta" and the third is "Block Annie Ta", with a sub-note below it stating "You and Annie will no longer be able to see each other or connect on Facebook". At the bottom right, there are two buttons: "Continue" and "Cancel".

3. Users also have the option to send a copy of the content to a trusted friend:

