



Reply Comments

of

The Association for Competitive Technology

on

COPPA Rule Review, 16 CFR Part 312, Project No. P-104503

December 23, 2011

The Association for Competitive Technology (ACT) thanks the Federal Trade Commission (FTC or Commission) for the opportunity to submit this reply to the Commission's September 27, 2011 Notice of Proposed Rulemaking (NPRM) to the Children's Online Privacy Protection Rule (COPPA).¹

ACT is an international advocacy and education organization for people who write software programs--referred to as application developers--and providers of information technology (IT) services. ACT represents over 3,000 small and mid-size IT firms throughout the world and advocates for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

Our goal is to help explain how small businesses that are fueling explosive growth in the mobile apps marketplace have become aware of their responsibilities under COPPA, how the rule changes outlined in the FTC's Notice of Proposed Rulemaking (NPRM) may affect them, and how small businesses are attempting to meet the goals of COPPA through innovation and parental outreach.

We repeatedly speak in public forums on the issue of protecting children with respect to technology and, more specifically, apps. We testified on the issue of child protection at the House Energy and Commerce Committee's hearing on "Protecting Children's Privacy in an Electronic World."² We served on a panel at the Family Online Safety Institute's (FOSI) annual conference addressing "How Do We Handle Apps?"³ Finally, we represent app developers similar to Moms With Apps, an online community of family-friendly developers, who have a particular interest in the outcome of the COPPA NPRM.

Overall, app developers have three key messages on COPPA and the NPRM:

- 1. The mobile apps ecosystem is creating American jobs and innovative new products, but heavy-handed new regulations could threaten that success.**
- 2. The NPRM demonstrates the power and the flexibility of the original COPPA legislation and proves that technology-specific privacy legislation is unwarranted at this time.**
- 3. The NPRM does a good job of clarifying and modernizing the original COPPA regulations. However, there are still areas where we think the FTC needs to expand examples of what is permissible and pull back from changes that could limit innovation.**

To support these messages, we provide case study examples of how apps and app developers will be negatively impacted by the NPRM.

The Smartphone Ecosystem is Creating Jobs and Opportunities in a Tough Economy

The evolution of mobile technology has led to a renaissance in the software industry; small software companies that once wrote exclusively for big software platforms at the enterprise level are now able to create innovative products and sell them directly to consumers. The emergence of the app market is a radical departure from the era of up-front marketing costs, publisher delays, and piracy. Its growth has eliminated the longstanding barriers to entry that our industry battled for the past two decades.

In the face of this tough economic environment, there has been a bright spot in the sales of smartphones and tablets, such as the iPhone, the HTC Thunderbolt (running Google Android), the Samsung Focus (running Microsoft WP7) and the Amazon Fire. These items continue to outpace all predictions and are providing a huge growth market in a slumping economy. Nearly one hundred million smartphones were shipped in the first quarter of 2011⁴ marking a 79% increase in an already fast growing market.⁵ In fact, 40% of adult mobile phone owners in the United States have smartphones. At the end of last year, smartphone sales were 20% of the U.S. market. Europe now sells more smartphones than feature

¹ Fed. Reg. 59804, Vol. 76 No. 187 (Sept. 27, 2011).

² U.S. House Energy & Commerce Committee, Hearing, Protecting Children's Privacy in an Electronic World (Oct. 5, 2011).

³ Family Online Safety Institute's Annual Conference, Panel, How Do We Handle Apps? (Nov. 9, 2011).

⁴ Mark Kurlyandchik, *IDC: Nokia Remains Top Smartphone Vendor Worldwide*, DailyTech, May 6, 2011.

⁵ *Id.*

phones.⁶

In 2008 Apple launched its App Store to provide a place for developers to sell independently developed applications for the iPhone. Since then, over one million new applications⁷ have gone on sale with billions of applications sold or downloaded. The Android platform has recently exceeded the growth rate seen in the iPhone, totaling more than 300,000 applications. In 2010 we saw the release of Windows Phone 7 with its own applications store and an entirely unique user interface. Recently, Microsoft released “Mango,” and Amazon launched the “Fire” tablet. Totally unique apps across all platforms continue to grow beyond the one million mark and the future looks bright.

The Mobile App World – A Job Growth Engine

The mobile app marketplace has grown to a five billion dollar industry from scratch in less than four years. In the next four, analysts expect that number to reach \$38 billion -- exceeding \$54 billion when including service expenditures.⁸

A recent study by the University of Maryland found the Facebook platform for app developers has created more than 182,000 jobs generating over \$12 billion in wages and benefits.⁹ Facebook is just one platform that app developers write for, with iOS, Android, and Windows Phone 7 also attracting mobile app developers. ACT’s own research estimates that the current mobile apps economy has created, saved, or supplemented more than 600,000 jobs nationwide.

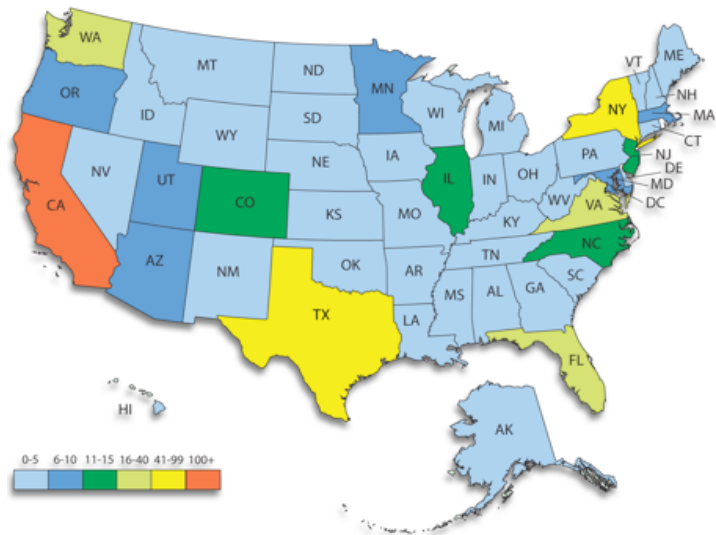
ACT regularly conducts workshops for app developer groups throughout the country, and we hear about opportunities for jobs in the app development world. And these aren’t just programmer jobs; app developers often need graphic artists, content writers, and marketers to assist in app development.

The jobs created by app development are not just in Silicon Valley. During the dot-com years, the majority of growth occurred in California while the rest of the country was not able to reap the direct benefits of the economic boom. However, today’s mobile apps industry is experiencing job creation across the country.

While California continues to have a large representation of app developers, nearly 70% of the businesses are located outside of the state of California. The nature of this industry allows developers to live almost anywhere, including: *Animal’s Pronunciations A to Z* by Rickety Apps in California, *Otto the Otter* by Baked Ham Games in North Carolina, and *Christ Church United Methodist* app by Speak in Tennessee.

Another feature of this new industry is that small businesses are the driving economic force. Of the 500 best-selling mobile apps, 88% are produced by small businesses.¹⁰ In a majority of cases these are micro businesses with fewer than 10 employees.

Developers of Top 500 Apps Across the Country



⁶ <http://www.engadget.com/2011/09/12/smartphones-out-ship-feature-phones-in-europe-samsung-leads-the/>

⁷ Shelly Freierman, *One Million Mobile Apps, and Counting at a Fast Pace*, N.Y. Times (Dec. 11, 2011).

⁸ http://blogs.forrester.com/john_mccarthy/11-02-28-mobile_app_internet_making_sense_of_the_2011_mobile_hysteria

⁹ http://www.rhsmith.umd.edu/digits/pdfs_docs/research/2011/AppEconomyImpact091911.pdf

¹⁰ ACT analysis of top 500 selling apps, some discrepancies exist due to lack of verifiable employment data and apps created by a developer who has significant investment from a larger company. Some apps branded for a larger company are in fact developed by small firms subcontracted to build the application. Sample size of 408 applications, from “top apps” on March, 25 2011.

How the NPRM Effectively Updates COPPA

The FTC has taken affirmative steps to update COPPA to changes in the technology marketplace. By clarifying and modifying existing law, this latest NPRM offers guidance to help app developers create quality content for children while protecting children's privacy.

Maintaining Consistency in the Age of Applicability

The FTC wisely maintained the existing age of COPPA applicability to those under 13. While increasing the COPPA age to 17 and under, as some had urged, would likely be found unconstitutional,¹¹ it would also upset the framework on which much of the Internet is based.

For example, many general audience Internet sites that collect personal information do not allow users under 13. If forced to comply with COPPA retroactively due to an increase in age, many users might suddenly find their access revoked. This could include access to cloud-based storage of their personal documents, social networking sites, and even sites as innocent as MovieFone.com and WashingtonPost.com.

Increased Clarity on COPPA's Application to Apps

The NPRM removes any uncertainty for mobile app developers about the applicability of COPPA and clarifies some key terms. While undefined by the original COPPA language, the NPRM provides certainty by identifying apps as an "online service." This helps us in our educational outreach efforts to increase awareness among our members of the need to comply with COPPA and to inform how they achieve compliance. However, while ACT appreciates the clarity the NPRM provides regarding unique identifiers' (UDID)¹² consideration as personal information (PI), we disagree with the NPRM's treatment of UDID as PI for the reason discussed in further detail later.

Increased Parental Notice is a Good Thing

ACT believes that transparency to the consumer is critical. Transparency informs consumers of how their information is being collected and used. This allows consumers to make educated decisions while eliminating the "scary factor." ACT has been very active in communicating to our developers the need to create and use privacy policies if their app collects personal information.

We do worry, however, that requiring too much disclosure results in diminished consumer awareness since warnings repeated too frequently are often ignored. Still, we are pleased to see the FTC's emphasis on empowering consumers to make informed decisions with greater transparency.

COPPA is aimed at protecting children's privacy online while increasing parental notice, consent, and involvement in how and when a child can share their information online. As app developers, this is also at the heart of the apps that we develop for children.

Challenges for App Developers

With every change, there are benefits and harms. We worry that in its effort to increase clarity, the FTC may have inadvertently created confusion for some app developers. This ranges from difficulties in app development and optimization to the inability to produce low cost, high quality apps for children.

Costs of Compliance with COPPA for App Developers

Too often websites and developers decline catering to those under 13 in order to avoid the difficulties and uncertainties of COPPA compliance. The requirements for parental consent are difficult and costly. Joining a safe-harbor program accompanies financial outlays. In fact, the Commission stated,

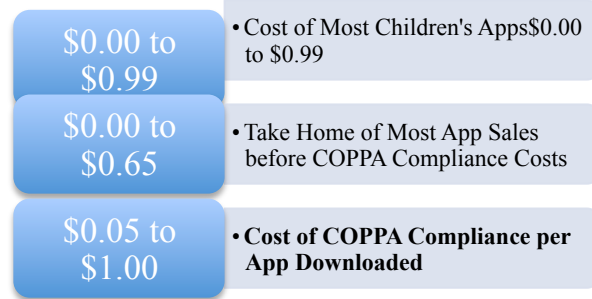
[I]t is unclear whether the economic burden on small entities will be the same as or greater than the burden on other entities ... in order to comply with the rule's

¹¹ See *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004) (upholding the injunction of enforcement of COPPA due, in part, to its applicability to those under 18).

¹² On an Apple product this is a combination of 128 letters and numbers.

requirements, *website operators will require the professional skills of legal ... and technical ... personnel ...* and that approximately 80% of such operators would qualify as *small entities* under the SBA's Small Business Size standards.¹³

As the number of children using computers, tablets, and smartphones increases, so do the opportunities to use these devices as learning tools. But to do so, there must be an economically viable platform on which these tools can be built. Current costs of acquiring parental consent range from \$0.05 to \$1.00 per app. Such a barrier is too high for many small businesses especially when most app developers net only \$0.65 or less per app sold. Accordingly, we ask that the Commission simplify compliance with COPPA and thus decrease the costs of compliance to these small entities.



Treatment of UDID as Personal Information – (CASE STUDY 1)

UDIDs provide many benefits to app developers while maintaining the anonymity of the person operating the device on which the app resides. For example, app developers often use a UDID for analytics purposes: seeing what parts of their apps kids like best or least, and using this information to improve their existing and future products. In fact, a recent focus group of app developers found that forty-four percent of them use analytics that rely on the collection of UDID to improve their apps.

Moreover, the UDID can be used to prevent unauthorized pirating of apps (ACT recently found that of the top ten apps on the iTunes store, Google searches on each returned downloadable copies within the top ten returned links¹⁴). All these benefits are achieved without the collection of any *real* personal information; the information contained in a UDID is used exclusively as a type of data-point.

While we at ACT think this collection falls under the “internal operations” exception, enough uncertainty remains to warrant further clarification. Moreover, the addition of unique device identifier (UDID) to the list of PI under COPPA creates unexpected consequences to app developers’ ability to improve and develop their apps.

We recognize that the FTC’s proposed definition of “support for the internal operations of the website or online service” includes “user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft.” However, we are uncertain if the collection for purposes of analytics invokes notice and consent requirements. Often the third-party terms-of-use allow the third-party to collect and store the UDID. With so few options for third-party analytics, app developers are stuck between non-negotiable terms of use and COPPA regulations. As an NPRM analysis by Cooley, LLP points out:

The FTC mentions parenthetically one example of a mobile application and an advertising network that collects information from within the application. No mention is given as to whether both the mobile application and the advertisement need to be directed toward children or whether both might be operators simply because either the mobile application or the advertisement is directed toward children. If the latter, this raises questions regarding whether parties have an obligation to conduct due diligence on the activities of the other party and the effect, if any, of contractual prohibitions on targeting children.¹⁵

A possible solution to this dilemma would be to expand the definition of “support for the internal operations of the website or online service” to explicitly include the collection for purposes of analytics even if by third parties.

¹⁴ This analysis was conducted using Google.com with the app name and the word “download.”

¹⁵ http://www.cooley.com/files/84589_ALERT_COPPAcoversMobile.pdf

An Unintended Consequence of Treatment of UDID as PI

App developers already feel the unintended consequences of the NPRM's change of PI to include UDID with the recent announcement from the analytics tracking company Flurry as the latest example. Flurry Analytics, the leading provider of app analytics, recently decided to discontinue its services for children's apps possibly as a result of the NPRM.¹⁶

This change is largely due to the alterations to the definition of PI to include the device identifier, IP address, and screen handles since the only allowance of the collection of this information without parental support is "for the internal operations of the website or online service." Further explained, these operations are defined to include only "those activities *necessary* to maintain the technical functioning of the website." Thus, while the information shared with Flurry is necessary to measure effectiveness and make improvements in the app, it is unlikely to be considered "support for the internal operations of the website or online service." Moreover, Flurry may want to use that information to improve their own product and to provide information to others about what people are interested in and on what they are focusing.

The FTC Should Not Treat UDID as PI Since the Drafters of COPPA Specifically Discounted Their Inclusion in the Definition of PI

Congress considered and dismissed including unique identifiers, like UDID, in the definition of PI in the original COPPA legislation. So the FTC's justification for the inclusion of UDID as PI, suggesting that Congress intended to include it in the original COPPA statute, is incorrect.¹⁷

IP addresses and persistent identifiers existed well before the creation of COPPA legislation. Moreover, privacy concerns regarding persistent identifiers were raised in the 1998 FTC Report to Congress¹⁸ on which much of COPPA's language is based.¹⁹ So when Congress wrote COPPA, it considered and dismissed IP addresses and persistent identifiers as PI. This conclusion is further bolstered by Congress's enumeration of PI criteria and specifically omitting persistent identifiers or IP addresses from that list.

Since the drafters of the COPPA legislation did not intend for UDID to be PI, the FTC should not make such a change at this point.

Treatment of User Name as Personal Information – (CASE STUDY 2)

A user name, like a UDID, without any other information is just a combination of letters and/or numbers. It does not necessarily identify any particular individual. Treating a user name as personal information has unintended consequences for app developers. Because app developers also rely on user names for analytics as opposed to UDIDs, the treatment of a user name as personal information limits their ability to provide useful educational and fun services to children.

ACT spoke with educational developers who are participants in Moms With Apps, a coalition of more than 600 moms (and now dads) who create educational apps. Several developers we spoke with noted that educational apps need to enable parents and teachers to see if children did their reading, took the test, or completed the project made available through the app. As part of the process to enable this review, the app creates user names for the children. If user names are considered PI, it could chill such innovation.

Prompting the Sharing of PI is Collection – (CASE STUDY 3 & 4)

While it may seem obvious that the prompting or encouraging of a child to share PI constitutes collection, the growth of social networking as a means to stay connected with kids and parents suggests a difference between "sharing" and "collecting."

¹⁶ "Our Customers may not use the Flurry Services in connection with any application labeled or described as a "Kids" or "Children" application and may not use the Flurry Services a) in connection with any application, advertisement or service directed towards children or b) to collect any personal information of children." <http://www.flurry.com/about-us/legal/privacy.html>

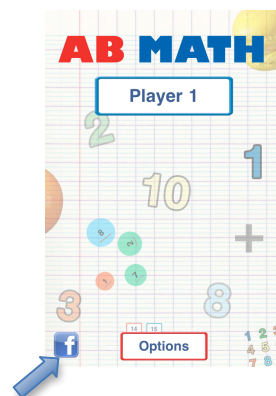
¹⁷ See, e.g. *id.* at p.33-34

¹⁸ Federal Trade Commission, *Privacy Online: A Report To Congress*, p.45-46 (June 1998), available at <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>.

¹⁹ See Congressional Record, 105th Congress, Senate p. S8483 (July 17, 1998) (citing the 1998 FTC Report to Congress as the rationale for introducing COPPA).

Social networking has changed the structure of nearly every app. “Like” and “Tweet This” buttons now persist across apps as diverse as cNet, Angry Birds, and Paper Camera. These buttons also exist on sites directed to children like AB Math.²⁰

These buttons allow all children to easily connect with their friends’ interests. However, the existence of these buttons may constitute a “prompting or encouraging of a child to submit personal information online”²¹ as defined in the “Collection” section of the NPRM since their presence “encourages” the sharing of PI. If an app “encourages” (which would be collecting under the NPRM) without prior parental consent, then the site violates COPPA. Since these buttons appear upon loading a webpage, there is no ability to obtain parental consent prior to this “encouragement” or sharing.



We do not believe that this is a scenario the FTC necessarily envisioned, but we ask that they review this outcome in the light of this limitation.

Imposing Data Requirements on Third Parties – (CASE STUDY 5)

Most app development is done by a small number of people utilizing collections of common code. In some ways, modern development practices are similar to building with Legos. Individual pieces may come in the form of “Software Development Kits”(SDK) and huge object code libraries found in common developer tools. But just like Legos, the developer is responsible for putting the pieces together in a unique and innovative way. This small-scale development is a core feature of app development and allows tiny one-man shops to develop software that rivals huge mega-corporations.

However, due to their small size, app developers often lack the ability to negotiate with the large companies whose tools or SDKs they must use, instead facing a take-it or leave-it contract. This makes asking app developers to impose any data storage or minimization requirements on larger companies unfair and unreasonable. By forcing app developers into this situation, we are left with two possible outcomes, one, large companies will not enter into contracts with app developers, or two, app developers will face sizeable legal burdens should the large third-party company violate COPPA.

Finally, small developers are in no position to mandate the disclosure of contact information, including phone number, for a large third party who provides needed services like analytics.

The FTC Should Not Discourage Forms of Parental Consent – (CASE STUDY 6)

Parental engagement is necessary for truly effective COPPA compliance and appears to be the goal of the statute. We want parents to know what their child shares online and we want them to be involved. Moreover, studies show parents *are* involved in granting consent to their child’s use of and sharing on apps,²⁴ although rarely is it COPPA compliant consent.

But when the FTC considers completely removing systems like email plus, it only discourages websites and developers from creating engaging, useful tools for children. This is especially the case when, as the FTC states, “few, if any, new methods for obtaining parental consent have emerged since the sliding scale was last extended in 2006.”²⁵ Alternative email verification services will not arise because of stricter COPPA guidelines – instead, we need to find ways to make parental consent simpler. That means not letting the perfect become the enemy of the good. Moreover, a recent study found that of the 12 year

²⁰ Facebook’s Terms of Service preclude its use by those under 13. However a recent study found that an overwhelming majority of parents consent, either explicitly or implicitly, to their under 13 year old being on Facebook. When app developers include “Like,” “Tweet,” and “+1” buttons parents are often the intended audience, but that does not preclude the reality that parents have often explicitly aided their children to set up Facebook accounts and therefore are using the feature. The same is true of services like Google’s “+1” and Twitter. See, e.g., Boyd, Hargittai, Schultz, & Palfrey, Why parents help their children lie to Facebook about age: Unintended consequences of the ‘Children’s Online Privacy Protection Act’, FM Volume 16, (Number 2011).

²¹ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.19-20.

²⁴ See, Lenhart, Madden, Smith, *et al.*, *How American teens navigate the new world of “digital citizenship”*, PEW Research Institute (Nov. 9, 2011).

²⁵ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p. 64 (FTC Notice of Proposed Rulemaking 2011).

olds on Facebook, 76% of parents helped their children sign-up²⁶ despite any COPPA violations. The study went on to state,

“Rather than providing parents with additional mechanisms to engage with sites honestly and negotiate the proper bounds of data collection about their children, parents are often actively helping their children deceive the sites in order to achieve access to the opportunities they desire. Were parents and their children able to gain access honestly, the site providers might well present them with child-appropriate experiences and information designed to enhance safety, provide for better privacy protections, and encourage parent-child discussions of online safety. With deception being the only means of access, these possibilities for discussion, collaboration, and learning are hindered.”²⁷

Clearly there is a disconnect between the consent of parents and their ability to grant that consent in a COPPA compliant way. So we believe the FTC should re-examine the elimination of email plus to determine if there are other ways to encourage innovation, including investigating alternative systems that are part of social network sites, game systems, and global marketplaces.

COPPA compliance is a substantial hurdle faced by small mobile app developers – who are challenged by screen size, business size, and evolving business models, but we are innovating and by innovating we can continue to develop educational tools to help children.

Purchasing an App with username and password should be a credit card equivalent – (CASE STUDY 7)

Presently, the FTC allows credit card transactions to constitute parental consent.²⁸ However, these transactions must be for a fee²⁹ paid through a credit card, and require the parent be notified in advance regarding the type of information collected.

The problem for app developers is that the regulations remain unclear as to whether financial transactions connected to a credit card authorized user account may fall within the existing form of parental consent. For example, when purchasing an app through the iTunes App Store, rarely is a credit card entered. However, to make any acquisition of an app, even a free app, the owner of the iTunes account’s password is required. This is akin to entering a banking account number or a credit card number.

The FTC should clarify that the purchase of an app using the password of an account tied to a credit card may be treated the same as if the credit card number itself were entered. Moreover, with most every app purchase, even for no fee, an email confirmation of the transaction is created and sent to the account holder. This allows parents to know what apps have been purchased and installed instantly rather than waiting for the monthly credit card bill. And since this receipt is created and the process is identical whether purchasing for a fee or free, the purchasing of free apps and free in-app purchases could constitute parental consent where the developer first provides notice. Simply put, the combination of clear notification plus the use of a username and password that is a credit card equivalent should be seen as verified parental consent.

Enable platform providers to obtain Parental Consent on behalf of App Developers

A number of practical COPPA compliance challenges arise from the fact that many apps are integrated into and operate through social media and mobile communications platforms that are maintained by a different operator. As a result, certain information, such as the user’s IP address, device ID, username or screen name, is sometimes shared between the app developer and the platform provider automatically when a user runs the application. This limited information sharing supports the technical and operational functioning of the app.

One alternative solution is to allow platform providers to offer notice and obtain consent on behalf of the app developer who offers access to online services through the platform. Under this streamlined

²⁶ Boyd, Hargittai, Schultz, & Palfrey, Why parents help their children lie to Facebook about age: Unintended consequences of the ‘Children’s Online Privacy Protection Act’, FM Volume 16, (Number 2011).

²⁷ *Id.* (emphasis added).

²⁸ 16 CFR § 312.5(b)(2).

²⁹ See FTC, *Frequently Asked Questions about the Children’s Online Privacy Protection Rule* (Oct. 7, 2008).

approach the platform operator would need to notify parents that multiple apps provide online services through the platform, generically describe the types of online services that these apps provide, and explain that these apps may collect and maintain the child's personal information to engage in "support for the internal operations" of the online service.

The platform operator would obtain verifiable parental consent that would cover the collection, use, and disclosure of the child's personal information by the platform provider and app developer, consistent with the disclosures made in the privacy notice. To the extent the app developer would like to use the child's personal information for purposes beyond support for internal operations, the app developer would be responsible for independently providing the parent with notice of these uses and obtaining verifiable parental consent consistent with COPPA.

This approach ensures that parents have meaningful notice of and control over how their children's personal information is collected, used, and disclosed online, without imposing unnecessary burdens and costs on app developers.

Conclusion

The apps ecosystem is creating innovative new products for teachers, parents, and children. Additionally, it is creating jobs. As the FTC considers the changes to COPPA outlined in the NPRM, we urge incredible attention to the potential risks of missteps that could cost small businesses and stifle innovation. Nonetheless, the FTC has made great strides at updating COPPA. Faced with an evolving marketplace that provides innovative ways to make learning fun, the Commission has taken a measured approach to improve child safety. While it requires additional changes, we are not suggesting the FTC throw the NPRM out with the proverbial bath water.

We concur with the FTC's frequent reminder to Congress that the Commission possesses sufficient existing regulatory authority to address online child safety. The strength of the COPPA statute and the flexibility of the regulatory process provide effective means to update the Act without the need for additional legislation.

We thank you again for the opportunity to submit this reply, and we look forward to working with the FTC in protecting children's privacy online as well as the innovators who are growing our economy.

Case Study 1: Treatment of UDID as Personal Information – Where's Mommy

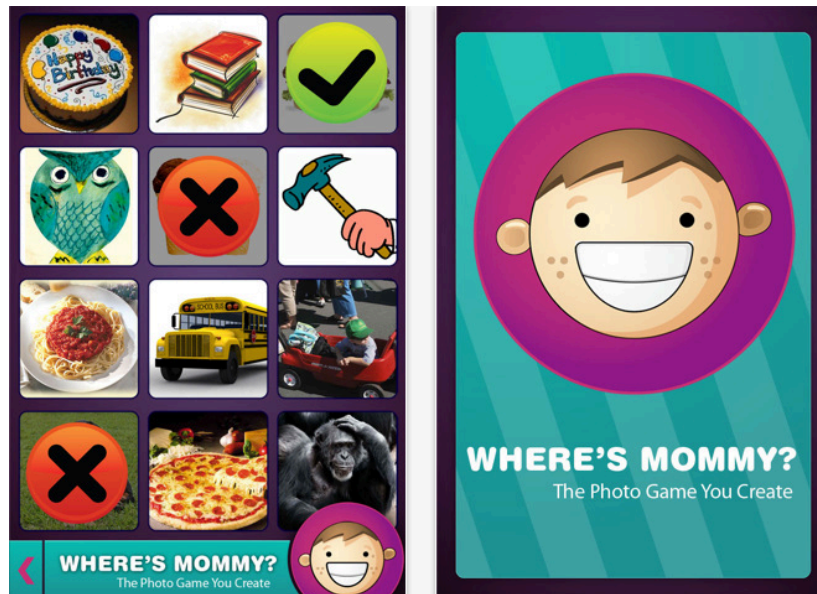
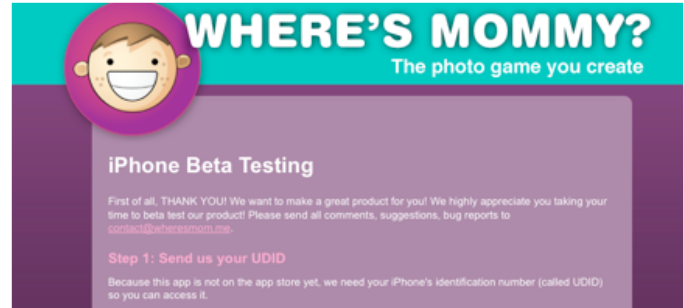
UDIDs allow app developers to anonymously trouble shoot and adjust their product before pushing it out to an app store.

What the app does: "Where's Mommy" is a kid's seek-and-match game that can be customized with your own photos and audio recordings. The game is similar to Where's Waldo, but it's more fun, educational and best of all, parents get to interact with children because they record the audio.

Children will really identify with the game and they'll learn new things, very fast.

How it uses UDIDs: Where's Mommy, by By Pitashi! was recently in "beta testing." While in beta testing, this app used UDIDs to: optimize its program, send copies of the app to beta participants, and ensure that no unauthorized copies were being installed.

Impact from NPRM: Under the NPRM, this process of beta testing is discouraged as many app developers will chose to deliver apps untested rather than risk legal liability through UDID based beta testing.



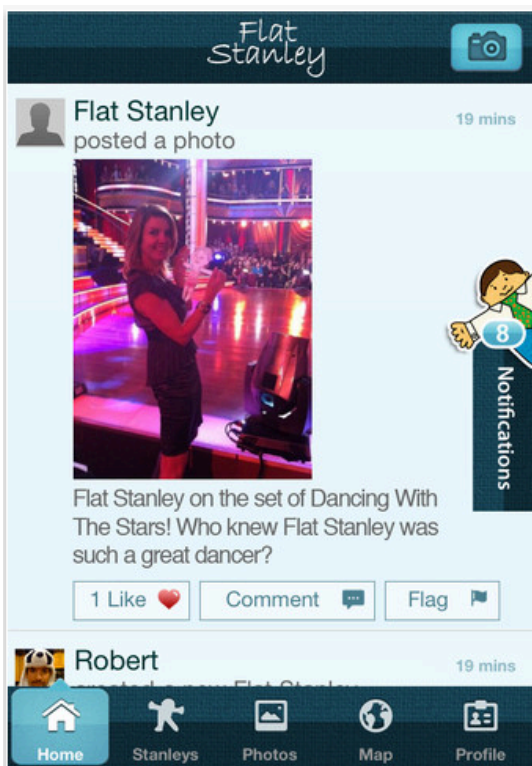
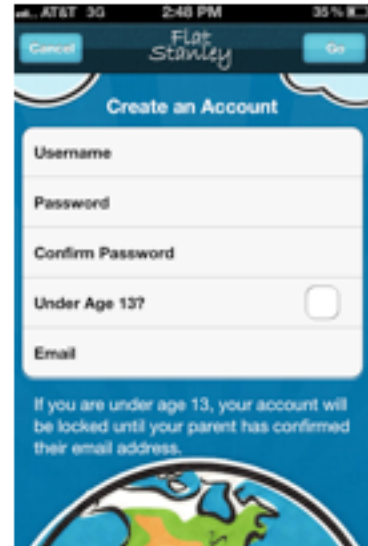
Case Study 2: Treatment of User Name as Personal Information – FlatStanley

Apps engage user names to increase connectivity and create app functionality.

What the App Does: A must have for anyone who has ever participated in the Flat Stanley Project. Since 1995 the Flat Stanley Project has been used by educators around the world to help children learn about travel, while discovering different cultures to develop a love for reading. This application makes it easier and safer for teachers, children and parents that want to create, travel and share their Flat Stanleys.

How it engages User Names: One of the ways Flat Stanley makes its services possible is through is through user names, asking for a username each time a child uses the app. This information does not permit the direct contacting of a child, just a way for the app to function.

Impact from NPRM: Under the NPRM, the core functionality of the app, the sharing of “Flat Stanleys” will be locked away behind a wall, rendering this app unusable to many of the children who love it.



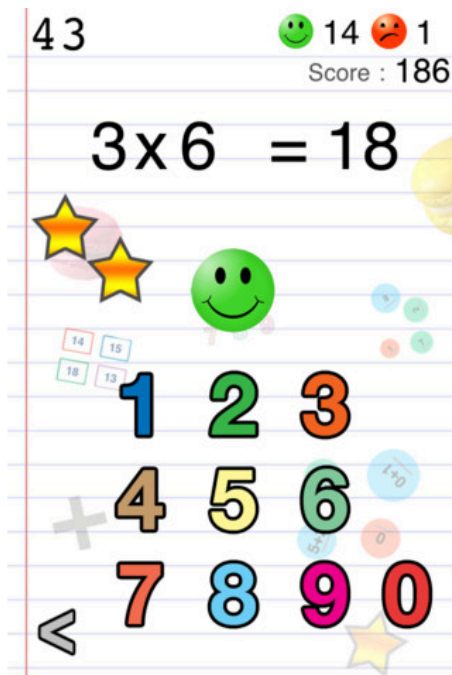
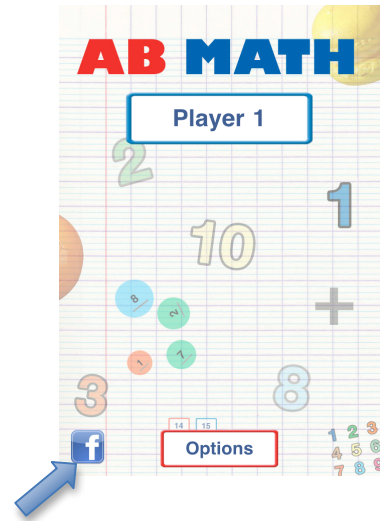
Case Study 3: App Developers Using “Like” Buttons Would Violate COPPA – AB Math

Facebook “Like” buttons allow app developers add in functionality and to better advertise their products.

What the App Does: Mental math game for kids from 5 to 10 : - The kids choose their options by themselves - Various fun game modes - Possibility to follow the results of several players - 4 levels of difficulty, including an EXPERT mode for grownups - Access to the Game Center - Mini games - The bubble game also strengthens sequential abilities, mental manipulation, attention and fine motor skills.

How it “Prompts or Encourages” Sharing: As the associated picture shows, AB Math has a Facebook “Like” Button attached to its app. This allows users to tell their friends that they “like” the app. Depending on the user’s Facebook privacy settings, “Liking” the app would make the user’s name or handle viewable to the app developer.

Impact of NPRM: If the NPRM considers the collection of PI to also include “prompting or encouraging” then the inclusion of the Facebook like button means that AB Math engages in collection of PI when a user first opens the app (since the button is shown when the landing page appears on the device). Under one possible interpretation of the NPRM, AB Math is “collecting” PI even before it has the opportunity to obtain parental consent.

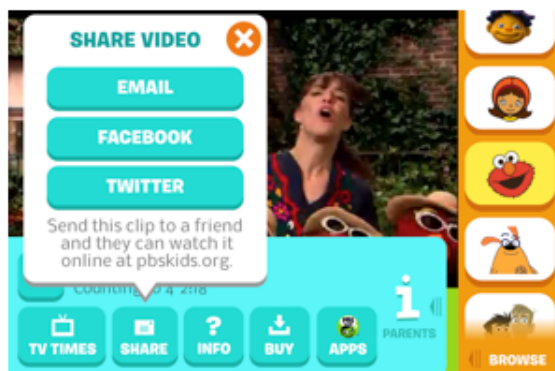


Case Study 4: Prompting the Sharing of PI is Collection – PBS Kids Videos

What the App Does: Watch videos from your favorite PBS KIDS television series anytime, anywhere (in the USA). “PBS KIDS Video” features more than 1,000 videos from over a dozen top PBS KIDS and PBS KIDS GO! television series, including Curious George, The Cat in the Hat Knows a Lot About That, Dinosaur Train, SUPER WHY!, Sesame Street and Wild Kratts.

How it “Prompts or Encourages” Sharing: On the PBS Kids Videos app, children can use email, Facebook, and Twitter to share videos and other services delivered through the app.

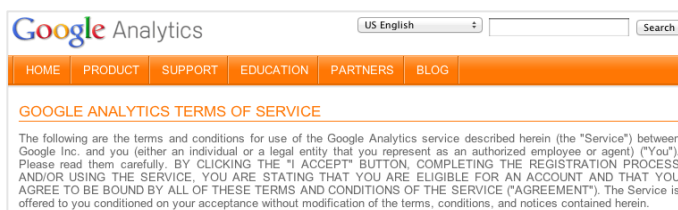
Impact of NPRM: PBS Kids Videos shows that almost any app is implicated by the NPRM’s “prompting or encouraging” language. While it is unlikely that the FTC intended to shut down apps and services to children like PBS Kids Videos, that would be the likely impact from the “prompting or sharing” language in the NRPM.³⁰



³⁰ Note it is possible that PBS kids would not be impacted by a post NPRM COPPA due to their status as a non-profit, however PBS has worked hard to follow COPPA and similar features are found on other privately created applications.

Case Study 5: The FTC Should Not Require App Developers to Impose Data Requirements on Third Parties

App developers are not in a position to negotiate with large third-party companies regarding data collection and storage requirements.



For example, the Google Analytics Terms of Service state, “The Service is offered to you conditions on your acceptance without modification of the terms, conditions, and notices contained herein.”

This is the type of “take it or leave it” contract that app developers face.

Hundreds of apps use services like Google Analytics – for example: “Color & Draw”

What the App Does: A complete art world for kids: color, play with stickers, or draw over photos!

Color & Draw is a complete artistic solution for TABLETS. It invites kids to draw, color and decorate drawings or photographs. Coloring pages have voice over invitations to get their creative juices flowing.

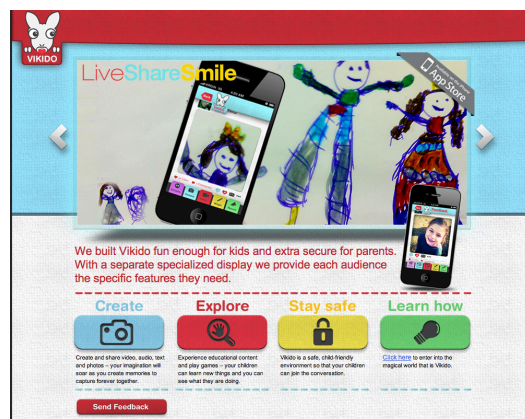


How the App Uses Analytics: TipiTap, the creators of “Color & Draw” use Google Analytics to measure the effectiveness of features in order to make improvements and measure how users value the app. Other analytics tools include an integrated error reporting and tracking system, which is vital for developers if a large number of errors are being reported from a particular device.

Impact of the NPRM: TipiTap does not have the size or scope to negotiate around a “take it or leave it” contract with Google regarding data treatment under COPPA. Instead, Google Analytics is more likely to deny its services to apps like TipiTap.

Case Study 6: Difficulty in Obtaining Parental Consent Using Existing Methods - Vikido

What the App Does: Vikido is a social sharing platform, designed for the web and mobile, that brings the entire family together in a fun, safe way. Through our no-reading required interface, Vikido is accessible to kids as young as four, and with clearly marked application buttons, you, the parent, know exactly how to maintain security and privacy for your family. With Vikido, children can create audio, video or pictographic content to share instantly with their parents. Parents can then decide exactly who views their child's creations--whether it be grandparents, a close contact from a limited list of your choice, or a broader, public circle via Facebook. Along with publishing creations, the Vikido Feed allows parents to 'Love,' comment and re-share posted content. It's a great way for grandparents to make sure they re-live every moment, aunts and uncles to stay in contact with nieces and nephews, and a wonderful way for cousins, brothers and sisters and close family friends to bond.



How the App Tries to Get Parental Consent: Vikido's mantra is "Create, Explore, Stay Safe." Children's safety is at the core of the Vikido application, highlighted from the very first screen. Vikido's privacy policy clearly states that no information from the child will be shared except through the parent account, and they've taken the time to explain COPPA to parents directly in their blog:

So, What is Vikido doing about this?

We started Vikido as "concerned parents" and that is why kids on Vikido don't have an "account" in the regular sense of the word – it's an extension of the parent's account. The parent logs in using FB connect, creates a "child" account – and the child is logged-in only via the parent's permissions – entering a child-mode interface.

So – no one can connect with your child unless you approve it (you add a family member via YOUR parent side, but the child doesn't have this ability).

In addition, no one can see the child's feed (other than his family) and the only person who can share the child's creations is the parent. You can see an example on my own facebook account: <https://www.facebook.com/amit.knaani/posts/10150310197421443> - that's me as a parent, sharing my child's pic under my name.

We also added an additional level of control by notifying the parent when a message is sent to the child.

"But it's kind of annoying to pay all that attention to my kids' activities!"

Well, the process implemented by Vikido requires at least some initial parental intervention and consent. The parent needs to register the child, add and approve other family members, and the child can't login with its own password. We know... it ain't easy, but we did it anyway, because just like you, we rather spend a couple of minutes here and there, and make sure we don't put our kids in harm's way.³¹

Impact of the NPRM: The NPRM is discouraging this kind of innovation. With the full understanding that it may require modification down the road, Vikido's efforts here are working to achieve exactly the desired outcome from COPPA: Parental understanding, engagement, and control. We ask that the FTC not only maintain the current models of parental consent, but also increase their availability.

³¹ See <http://vikido.com>

Case Study 7: Purchasing an App Should Be Part of Verifiable Parental Consent, Even if Free – Amazon App Store

Amazon.com makes available an app store. Any purchase through this store is through the associated Amazon.com account. This Amazon.com account is connected with a credit card kept on file, and requires the entering of a password for each transaction, even when the total cost is \$0.00.

In addition to requiring a credit card on file, and the entry of a the account password for each transaction, Amazon.com produces and emails a receipt of any app purchased, free or for cost, to the owner of that Amazon.com account. This provides security to parents that their children cannot install apps from the Amazon.com App store without parental consent and a credit card. And in the event that an app is installed, the parent receives written notice of such an installation.

Amazon.com is not alone as most all app stores engage in the same or similar process. This way the parent is always aware of what apps their child has access to, whether acquired at no cost, or for a dollar.

Since this receipt is created and the process is identical whether purchasing for a fee or free, the purchasing of free apps and free in-app purchases could constitute parental consent where the developer makes clear, either through the description page of the app or through the pre-installation properties tab, the kind of sharing that will be done.

The combination of clear notification plus the use of a username and password that is a credit card equivalent should be seen as verified parental consent.

Your Amazon.com Order (D01-8512223-5391916)
1 message

Amazon.com <digital-no-reply@amazon.com> Wed, Dec 7, 2011 at 10:18 AM
Reply-To: Nobody <digital-no-reply@amazon.com>
To: " " <@gmail.com> " <@gmail.com>

amazon.com. [YOUR ACCOUNT](#) | [HELP](#)

Thanks for your order,

Did you know you can view and edit your orders online, 24 hours a day? Visit [Your Account](#).

Reading from a mobile device? [Open the Amazon Appstore for Android](#) or download it to your device.

Order Information:
E-mail Address: [@gmail.com](#)
Billing Address:

WASHINGTON, DC
United States
Phone:

Order Grand Total: \$0.00
Earn 3% rewards on your Amazon.com orders with the Amazon Visa Card. [Learn More](#)

Order Summary:
Details:
Order #: [D01-8512223-5391916](#)
Subtotal of Items: \$0.00

Total before tax: \$0.00
Tax Collected: \$0.00

Total for this Order: \$0.00

The following item is available now. See all your apps and registered devices in [Your Apps & Devices](#).
Pocket Informant [Apps for Android] \$0.00
Sold By: Amazon Digital Services, Inc.

You can review your orders in [Your Account](#). If you've explored the links on that page but