**Protecting Children Online and On Mobile**
**Commissioner Terrell McSweeny**
CARU Annual Conference Keynote Speech
Wednesday, October 1, 2014

Thank you, Lee, for that kind introduction, and thank you so much for inviting me to be here today. I'm delighted to have the opportunity to speak to you. As many of you know, I am the newest FTC Commissioner -- I was sworn in only a little over five months ago.

I've enjoyed joining the Commission during its centennial. Last Friday we celebrated the 100th anniversary of President Woodrow Wilson's signing of the FTC Act. As I was tweeting about it, I couldn't help but wonder what Wilson would make of smartphones and apps. While he and the architects of the FTC could not have anticipated all the innovations of our mobile, highly connected 21st century economy, I think they certainly did appreciate that the FTC's mission to protect consumers and competition would evolve along with the economy. That's what I'd like to talk to you about today: how our shared interest in protecting children is evolving.

First, full disclosure. I have a personal interest in this topic – not just as an FTC Commissioner, but as a mom of two small children. I have first-hand experience raising tech-savvy digital natives who are consuming media in all kinds of new ways. I want them to benefit from all of the advantages that technology has to offer – at the same time, though, I worry about the trail of digital footprints they might be leaving behind and how they are being influenced by the messages conveyed in advertising and media.

Protecting children is not just a personal priority of mine – and of yours – but it's also a priority of the entire Federal Trade Commission. All of our efforts to protect children are connected by a central theme: Parents and caregivers should be provided with truthful and adequate information so that they can make meaningful choices for their children. You can see this clearly in some of our recent enforcement actions and in our administration of the COPPA Rule.

Earlier this year, we announced settlements with both Apple and Google relating to unauthorized purchases made by children in mobile apps, and we have a pending case against Amazon on the same issue.

Smartphones and tablets are irresistibly attractive – and now ubiquitous – sources of entertainment for children, and many mobile app developers have created games and activities that are geared specifically to kids. For instance, you can download games where your children can raise virtual pets, clothe virtual dolls, or play in Smurf Village. Many of these games are available for free, so often parents will download them from app stores and then hand their phone or tablet over to their children to play. I speak from personal experience.

Some of these games include the ability to use virtual money to buy virtual products – for instance, food to feed your virtual pet. But some games also allow users – including children –

to spend real money on virtual goods. They invite children to obtain virtual items in contexts that blur the line between what costs virtual money and what costs real money.

For example, the "Air Penguins" app invites children to journey through the icy South Pole to help an animated penguin save his family from melting ice caps by jumping from iceberg to iceberg. The game includes a screen selling polar bears, penguins, and various quantities of fish. The screen does not contain any dollar signs or other description of the real-money cost of any of the items. Buying polar bears and penguins costs virtual currency, but buying fish costs real money, with the largest available quantity of 20,000 fish carrying a price tag of $49.99.

As another example, the Ice Age Village app lets children manage an ice-age habitat, with instructions offered by characters from the animated "Ice Age" movies. The in-game "Shop" offers virtual items such as animal friends, buildings, or more land, each of which cost a certain amount of virtual currency – either "coins" or "acorns." When children purchase these virtual items, there is no real-money charge. But when children purchase the coins or acorns, they are charged real money, and the largest quantities (4,200 acorns or 2,100,000 coins) will set them – or rather, their parents! – back $99.99.

Of course, there's nothing wrong with a mobile app providing the capability to make purchases with real money. Developers who offer their apps at no cost often need to find a way to monetize their offerings, whether it's through advertising or in-app purchases. But what is a problem is when consumers are not given adequate notice of the fact that such in-app purchases are available, and when children are able to go on spending sprees without even needing to input a password.

For instance, in the FTC's case against Apple, we alleged that although parents were prompted for a password when a child wanted to make an in-app purchase, inputting the password opened up a 15-minute window of time when children could make additional, unlimited purchases, without the need to enter a password again. Because some in-app purchases are quite expensive – $10, $20, or even $100 – children can rack up enormous bills for in-app purchases totaling hundreds of dollars, even in just 15 minutes.

In our case against Google, we alleged that when the company first started offering apps, it didn't require a password at all to make in-app purchases. The company changed this policy more than a year later to begin requiring a password, but parents who entered the password opened up a 30-minute window of time for additional, unlimited purchases. In both cases, parents who sought refunds for such purchases faced obstacles, such as a "no refund" policy or being referred to the app developer for a refund, an exercise that was often futile.

I'm pleased with the resolution to these cases. Not only have Apple and Google agreed to provide millions in refunds for unauthorized in-app purchases by children, they are also improving notice and consent policies. Apple has added a popup box to the in-app purchase flow. The pop-up informs consumers of the 15-minute billing window and gives them the choice of whether to accept or reject it. Our order with Google is not yet final, but the proposed order requires the company to get informed consent for in-app charges, while giving the company flexibility in how it wants to implement that requirement.

I want to stress that the FTC is not trying to minimize how important it is for parents to be engaged with how their children use technology and to monitor their use. It's also critical for parents to talk to children about their expectations and rules for what content children will be allowed to access, for how long, and any other limits the parents want to set. But the way that the in-app purchases were presented undermined parents' ability to have meaningful control.

In many cases, when parents downloaded a free game, they were unaware of the fact that it even offered their children the opportunity to make in-app purchases that would cost real money.

Even if children knew they were not supposed to make purchases without permission, they might not have been able to distinguish between items that cost virtual currency and purchases that cost real money, so they could have unwittingly made real money purchases without realizing they were doing so. And the failure to inform parents that inputting a password would open up a significant window of time to make additional, unlimited purchases ultimately denied parents the information they needed to be able to take whatever steps they deemed appropriate to control their children's spending – such as approving every single purchase, or engaging parental controls to disable such purchases altogether.

I also want to mention another recent FTC enforcement action: our case against Snapchat. Snapchat is a hugely popular mobile app that promised users that photos and videos sent to friends through the service would permanently disappear, after no longer than 10 seconds. As of last fall, consumers were sending 350 million "snaps" daily. The company agreed to settle charges that its promises that messages would disappear forever were deceptive, in addition to other allegations relating to the collection of geolocation and other personal information, and the failure to properly secure information to protect it from unauthorized access.

Snapchat was not targeted to children, but the reason I mention it is because mobile apps like Snapchat are often disproportionately popular with youth – while perhaps not with the under 13 crowd, but certainly with teens and adolescents who are more likely to have their own smartphones. According to media reports, 50% of Snapchat users are between ages 13 and 17. It's easy to see why the app would appeal to younger users, who tend to be less inhibited online and potentially more emboldened to send content to others, especially when they are promised that the content will be ephemeral.

The popularity of Snapchat among young adult users is a reminder that parents need to continually engage their kids about online safety and appropriate behavior, beginning from an early age and continuing through the tween and teen years. The FTC offers some fantastic consumer education resources about how to have these conversations, such as our NetCetera booklet that gives guidance on topics like parental controls, social media, cyberbullying, mobile devices, and computer security. Like all of our publications, NetCetera is available for free, and we have distributed over one million copies of it just since the beginning of the year.

The FTC also makes protecting children a priority through its administration and enforcement of the Children's Online Privacy Protection Act Rule. The COPPA Rule gives

parents control over the personal information collected online from their children. As I'm sure all of you are aware, the Commission finalized amendments to the COPPA Rule at the end of 2012, with the changes taking effect in July 2013. When the Commission first promulgated the COPPA Rule in 1999 – requiring parental consent for the online collection of personal information from children under 13 – the internet was a vastly different place, including the manner and extent to which children utilized online and mobile services. The updates were meant to modernize the Rule, taking into account newer technologies and business models, such as the use of behavioral advertising.

Now I know there is a lot of discussion going on regarding the particulars of how to comply with the modified Rule – in fact, I noticed it was the topic of an entire panel this morning. What I want to emphasize is that the FTC wants to work with industry and stakeholders to provide useful guidance and advice as to how to comply with the Rule. Our staff attorneys maintain and update a very comprehensive FAQ on how to comply with COPPA. Some of the most recent additions to the FAQ include information on how entities such as app stores could provide verifiable parental consent mechanisms for app developers operating on their platforms.

Since we amended the COPPA Rule, the Commission has approved two new COPPA Safe Harbor programs (and I would be remiss if I didn't acknowledge that of course CARU was the very first Safe Harbor program), bringing the total of approved programs up to seven. Another revision in the Rule provides a formal mechanism to obtain Commission approval for new methods of verifiable parental consent. We have received several applications and approved one. We hope that the industry will continue to innovate and come up with new methods of parental consent that will facilitate compliance with the Rule.

We continue to vigorously enforce the COPPA Rule. Just a few weeks ago, we announced settlements with Yelp and TinyCo to resolve COPPA violations. Yelp, of course, is not a child-directed site. But our action against Yelp is a good reminder that COPPA applies to operators of general interest websites and online services who have actual knowledge they are collecting information from children under 13. The case is also a reminder that it's just as important to keep privacy in mind for mobile apps as it is for websites.

While Yelp had an effective age screen for its website that prevented children from registering, we alleged that Yelp accepted registrations on its Apple and Android mobile apps from users who supplied a date of birth indicating that they were under the age of 13. Users who registered provided other information covered by the COPPA Rule, including their first and last name, email address, and ZIP code. After registering, users had full access to Yelp, including the ability to upload photos, indicate their current city, provide information in free-form text fields, and "check-in" at local businesses. Further, Yelp automatically collected the Mobile Device IDs of all app users, as well as geolocation information from users who granted Yelp permission to do so.

Our case against TinyCo involved a developer of mobile apps directed to kids, such as "Tiny Zoo," where players collect, feed, and breed animated animals to build a zoo. We alleged that TinyCo collected tens of thousands of email addresses from users, including from some

users who received free in-app currency in exchange for providing the address. We further alleged that TinyCo received complaints from many parents whose children under the age of 13 were using the apps, and that the company did not take steps to determine whether it was in compliance with COPPA after receiving such information.

I want to assure you that while the Commission wants to ensure that the COPPA Rule provides strong privacy protections for children, at the same time we recognize the value in promoting innovation to encourage development of varied and vibrant choices in online content and activities for children. Therefore, we will continue to work with industry to find ways in which we can achieve both of these goals.

While we generally think of the COPPA Rule as a privacy regulation – after all, it is the implementing rule for the Children's Online Privacy Protection Act – the COPPA Rule also has a data security component that is often overlooked. In fact, the Rule includes a provision requiring operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity" of personal information collected from children. The recent amendments to the Rule expanded this provision, requiring operators to release children's personal information only to companies that are capable of keeping it secure and confidential, and that provide assurances they will do so.

In our COPPA case against RockYou in 2012, we alleged that RockYou violated this provision of the Rule – among others – when it stored passwords in clear text and failed to protect its website from commonly known or reasonably foreseeable attacks, resulting in a breach that compromised 32 million email address and passwords. It makes perfect sense that the COPPA Rule has a data security requirement, because you cannot have privacy without data security. Unfortunately, it's easy for data security to be overshadowed by or conflated with the concept of privacy.

Privacy is about what companies are intentionally doing with consumer information. Consumers want to know… Is my information being collected? Is it being stored, and for how long? Why? Is it being sold or shared? And to whom? Am I being tracked as I surf the web and use my mobile phone? Is someone compiling a dossier of my shopping habits? Do I have the opportunity to say no to any uses of my information?

Data security, on the other hand, is about what a company is doing to protect your information from outsiders, like hackers and thieves. You can have a company that has wonderful privacy practices – clearly telling you what information it's collecting and with whom it's shared – but what if that company has your credit card number and is not doing enough to protect it from hackers?

Data security is often invisible to consumers. It is generally impossible for a consumer to gauge whether or not her information is being adequately protected. And it can be impossible to predict – who knows which company will be breached tomorrow?

The reason I think data security is so important is that a company can make all the promises in the world about what information it's collecting, but if it doesn't keep that

information secure, then its promises are all for naught. This is one of the reasons that the Commission unanimously supports comprehensive data security legislation that would require companies to have reasonable data security measures. Data security is not a one-size-fits-all issue – the level of security you must have depends on the size and capabilities of your organization, and the sensitivity of the information that you are safeguarding. But I would suggest that information collected from and about children falls into the category of information that merits special care and protection.

I want to close by acknowledging CARU and all of the programs under the Advertising Self-Regulatory Council for the important work you do in monitoring and policing advertising. The Commission strongly supports self-regulation. The ASRC programs provide an effective and efficient forum to resolve many advertising issues and competitive disputes, including in some areas where the FTC does not have enforcement authority, such as CARU's Children's Food and Beverage Advertising Initiative, which establishes voluntary nutritional standards for the advertising of food to children. We know that CARU's uniform nutritional guidelines took effect at the beginning of the year, and we are looking forward to seeing how this impacts food advertising to children. We hope to see continued progress on this front.

With that, I'll end, and I am happy to take any questions.