Family Online Safety Institute Annual Conference, "Redefining Online Safety"
November 12, 2014
Washington, D.C.
Remarks of Commissioner Terrell McSweeny

Thank you so much, Pat, for that very nice introduction. I'd also like to thank FOSI for inviting me to be here today. It's a pleasure to have the opportunity to talk to all of you about the FTC's work to protect children in a networked, data-driven world.

It so happens that the FTC is celebrating its 100th anniversary this year, and many of us at the Commission have been reflecting upon how the agency's work has evolved over time. In preparation for speaking with you today, I did a little research into the origins of the FTC's work on children's privacy. Protecting children from unfair or deceptive marketing has long been a part of the FTC's consumer protection mission. Almost twenty years ago, the FTC began studying the impact of the then "new" online marketplace on consumer privacy – including privacy of children.

In 1998 the FTC surveyed several hundred websites collecting personal information from children and found a range of practices that I think, today, we would all agree are troubling. For example, the FTC found a website where children could seek electronic pen pals by posting a message with their email address. To register on some sites children were asked to provide their full name, mailing address, birthdays, and hobbies. On other sites, children encountered imaginary characters who solicited information from them. One site in the survey even asked children personal financial questions like: "Do you own mutual funds? Are your parents currently saving for your college education? What do you usually do with gifts of money?"

In some cases these sites contained information practice disclosures – but they contained statements like this: "Kids, get your parents' permission before you give out information online." Just one percent of the sites actually required parental consent before information was collected from a child. Parents were concerned. Protections for kids online were very uneven. The FTC concluded that self-regulatory initiatives were not sufficiently protecting children's online privacy and recommended that Congress enact legislation. The Children's Online Privacy Protection Act (COPPA) was passed in 1998 with bipartisan support.

Today this anecdote seems like ancient Internet history. But allowing parents to make informed choices about when and how their children's information is used and collected is just as – perhaps more – important today in our increasingly networked world.

As the mother of young children who, at four and six years old, are already tech-savvy, I have a personal appreciation for how difficult it is for parents to navigate protecting their children while also allowing them to engage with all the wonderful innovations that are literally at their fingertips. As we confront new issues – like how best to protect student privacy or how to manage the privacy and security of kids growing up with wearables, mobile devices and connected toys – it is important to remember that parents are the front lines when it comes to helping children make good choices about technology, or recover from bad ones. And we need

all the help we can get – which is why it is terrific that resources like FOSI's Good Digital Parenting initiative are available.

The FTC helps parents in a variety of ways – by providing resources, like our NetCetera guide, which explains different types of parental controls and encourages parents to talk to kids about being online, and by taking law enforcement action when parents are not provided with truthful or adequate information.

Earlier this year, the FTC 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. In these cases, we found that parents often download mobile apps for their children that are advertised as free, without being aware of the fact that many free apps provide the opportunity to make purchases within the app using real money. For instance, an app might allow a child to raise a virtual pet by feeding it virtual food that costs real money. Or a game may allow a player to buy some items with virtual currency and others with real money, blurring the line between purchases that are imaginary and those that will end up on mom and dad's credit card bill.

There's nothing wrong with the practice of in-app purchases in and of itself. The crux of the problem in these cases was that consumers – meaning the parents who were paying the bills – were not adequately informed of the fact that the apps their children were using included in-app purchase capabilities, and they were not adequately informed when children were actually making purchases, or how much these purchases cost. Without this information, even parents with the best intentions of supervising their children's use of the apps were not equipped to prevent them from going on in-app spending sprees of hundreds, or even thousands, of dollars. As a result, under the terms of their settlements, Apple and Google will provide tens of millions of dollars in refunds to parents. Our litigation with Amazon is still ongoing.

The FTC also takes enforcement action when users are misled about the privacy or security of an app or online service. For example, in our case against Snapchat, an app that is disproportionately popular with teens, the company agreed to settle charges that it deceptively promised that messages would disappear forever, and that it failed to properly secure information and protect it from unauthorized access. Cases like this are particularly important because it is vital that parents and teens have truthful information about privacy and security when making decisions about whether to use an app or social networking site.

This is especially true as we increasingly introduce a range of connected devices into our homes. Last year, the FTC brought its first case involving an "Internet of Things" device against TrendNet, a company that sold Internet-connected home security cameras. Consumers could monitor their homes remotely on a computer or smartphone, but the company's lax security procedures exposed the private video feeds of hundreds of consumers to public viewing on the Internet, even when consumers had taken steps to password protect them. These feeds displayed babies asleep in their cribs, children playing, and adults going about their daily lives. Our settlement with TrendNet requires the company to establish a comprehensive information security program that will assess risks, design and implement reasonable safeguards to address those risks, and regularly test, monitor, and adjust security measures – a model for how

companies making Internet-connected devices for the home can go about insuring these devices are secure.

Finally, the FTC also makes protecting children and parental control a priority through its administration and enforcement of COPPA. The Commission finalized amendments to its COPPA Rule at the end of 2012, and these changes took effect in July 2013. I know that some stakeholders, including FOSI, have raised concerns regarding the cost and difficulty of compliance with the newly amended Rule. The FTC absolutely recognizes the value of having a rich and varied selection of online content for children. We are not trying to impede innovation in this space. Our goal is to work collaboratively with industry to help members comply with the COPPA Rule. We have recently approved two new COPPA Safe Harbor programs, bringing the total number of approved programs up to seven. And we hope that industry will come up with new methods to facilitate parental consent. One revision in the Rule provides a formal mechanism to obtain Commission approval for new methods of verifiable parental consent, and I think we will see promising innovations in this area.

We continue to vigorously enforce the COPPA Rule. We recently announced settlements with Yelp and TinyCo to resolve COPPA violations. Yelp had actual knowledge it was collecting personal information from children under 13. Although Yelp did not allow children to register on its website, we alleged that the company accepted registrations from children on its Apple and Android mobile apps. Children who registered provided their first and last name, email, and ZIP code, and were to upload photos, provide information in free-form text fields, and "check-in" at local businesses. Yelp also collected the Mobile Device IDs of all app users, and geolocation information from users who gave the company to do so.

Our case against TinyCo alleged that the mobile app developer collected tens of thousands of email addresses from users of its apps, such as "Tiny Pets," "Tiny Village," and "Tiny Monsters." These apps were directed to children and TinyCo was aware that children under 13 were using them. But even after receiving complaints from many parents whose children were using the apps, the company did not take steps to determine whether it was collecting personal information without parental consent.

Parenting in the digital age – weighing the potential benefits and harms of new technology to children – can be confusing. I recognize that when it comes to privacy and data security, there is no one-size-fits-all solution. But I hope that we can all agree that parents should have the tools they need to protect their families and to make informed choices about when and how information is collected from their children.

Thank you again for having me here today.