PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

"PROTECTING YOUTHS IN AN ONLINE WORLD"

SUBCOMMITTEE ON CONSUMER PROTECTION,

PRODUCT SAFETY, AND INSURANCE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, DC

July 15, 2010

I. INTRODUCTION

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect the privacy and security of teens in the digital environment.

The Federal Trade Commission is committed to protecting teens as they navigate digital technologies and applications. The agency has actively engaged in education, law enforcement, and policy efforts to help make the digital world safer for all consumers, including teens.

This testimony first highlights some of the privacy and safety risks teens face as they participate in the digital world. Second, it summarizes the Commission's efforts to educate teens and their parents about these risks. Third, it highlights the Commission's efforts to protect privacy in the context of technologies used heavily by teens in particular – social networking, mobile computing, and peer-to-peer ("P2P") file-sharing programs. Finally, the testimony addresses proposals to create separate privacy protections for teens online.

II. TEENS IN THE DIGITAL ENVIRONMENT

Teens are heavy users of digital technology and new media applications including social networking, mobile devices, instant messaging, and file-sharing. Indeed, a 2007 study found

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

that over 90 percent of kids between the ages of 12 and 17 spend time online.[2] The online world has changed how teens learn, socialize, and are entertained. In many ways, the experiences teens have online are positive – they use the Internet to socialize with their peers,[3] to learn more about topics that interest them,[4] and to express themselves.[5]

But teens also face unique challenges online. For example, research shows that teens tend to be more impulsive than adults and that they may not think as clearly as adults about the consequences of what they do.[6] As a result, they may voluntarily disclose more information online than they should. On social networking sites, young people may share personal details that leave them vulnerable to identity theft.[7] They may also share details that could adversely

---

[2] Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), *available at* www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

[3] *See* Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), *available at* www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/More-details-from-the-survey.aspx?r=1.

[4] *See* Kaiser Family Foundation, *Generation M2: Media in the Lives of 8- to 18-Year-Olds* (Jan. 2010), *available at* www.kff.org/entmedia/upload/8010.pdf.

[5] *See* Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), *available at* www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1.

[6] *See, e.g.,* Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, *available at* htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031710_sess3.pdf; Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), *available at* ssrn.com/abstract=1589864.

[7] *See* Javelin Strategy and Research, 2010 *Identity Fraud Survey Report* (Feb. 2010), *available at* www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf.

affect their potential employment or college admissions.[8] Teens also sometimes "sext" to their peers – send text messages and images with sexual content – without considering the potential legal consequences and harm to their reputations. According to one recent study, 4 percent of cell phone owners aged 12 to 17 have sent sexually suggestive images of themselves by phone, while 15 percent have received "sexts" containing images of someone they know.[9] In addition, bullies or predators – most often teens' own peers – may try to take advantage of adolescents on the Internet. About one-third of all teens online have reported experiencing some kind of online harassment, including cyberbullying.[10]

Despite teens' sharing and use of personal information in the digital world, there is data that suggests teens are concerned about their online privacy. For example, one study of teens and privacy found that teens engage in a variety of techniques to obscure or conceal their real location or personal details on social networking sites.[11] The Commission seeks to address these privacy concerns – as well as parents' concerns about their teens' online behavior and

---

[8] *See e.g.,* Commonsense Media, *Is Social Networking Changing Childhood? A National Poll* (Aug. 10, 2009), *available at* www.commonsensemedia.org/sites/default/files/CSM_teen_social_media_080609_FINAL.pdf (indicating that 28 percent of teens have shared personal information online that they would not normally share publicly) .

[9] Press Release, Pew Internet & American Life Project, *Teens and Sexting* (Dec. 15, 2009), *available at* www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx.

[10] Amanda Lenhart, Pew Internet & American Life Project, *Cyberbullying and Online Teens* (June 27, 2007), *available at* www.pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf.

[11] Amanda Lenhart and Mary Madden, Pew Internet & American Life Project, *Teens, Privacy, and Online Social Networks* (Apr. 18, 2007), *available at* www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1.

interactions – through education, policy development, and law enforcement, as discussed further below.

III. CONSUMER EDUCATION

The FTC has launched a number of education initiatives designed to encourage consumers of all ages to use the Internet safely and responsibly. The Commission's online safety portal, OnGuardOnline.gov, developed in partnership with other federal agencies, provides practical information in a variety of formats – including articles, game, quizzes, and videos – to help people guard against Internet fraud, secure their computers, and protect their personal information.[12] The Commission's booklet, *Net Cetera: Chatting With Kids About Being Online*,[13] is the most recent addition to the OnGuardOnline.gov consumer education campaign. This guide provides practical tips on how parents, teachers, and other trusted adults can help children of all ages, including teens and pre-teens, reduce the risks of inappropriate conduct, contact, and content that come with living life online.

Net Cetera focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy. It provides specific advice to parents about talking to their children about each of these topics. For example, on the subject of sexting, it discusses the risks sexting poses to kids' reputations

---

[12] The OnGuardOnline.gov website is the central component of the OnGuardOnline consumer education campaign, a partnership of the federal government and the technology community. Currently, 13 federal agencies and a large number of safety organizations are partners on the website, contributing content and helping to promote and disseminate consistent messages. Since the launch of OnGuardOnline.gov and its Spanish-language counterpart AlertaenLínea.gov in September 2005, more than 12 million visitors have used these sites for information about computer security.

[13] *NetCetera* is available online at www.onguardonline.gov/pdf/tec04.pdf.

and friendships – as well as possible legal consequences if kids create, forward, or save these kinds of messages – and gives parents straightforward advice: "Tell your kids not to do it." With respect to cyberbullying, *Net Cetera* advises parents to talk with their kids about online behavior and about any messages or images that make them feel threatened or hurt. The guide advises parents to work with a child who is being bullied by helping them to not react, save the evidence, and block or delete the bully.

The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera*, and the agency has distributed more than 3.7 million copies of the guide since it was introduced in October 2009. The FTC will continue to work with other federal agencies, state departments of education, school districts, and individual schools to distribute *Net Cetera* and OnGuardOnline.gov to parents and educators. Additionally, the FTC plans to reach out to other groups that work with kids, such as summer camps, state education technology associations, and scouting organizations to publicize these materials.

In furtherance of the FTC's education efforts, Commission staff also participated in the Online Safety and Technology Working Group (OSTWG), a working group composed of private sector members and federal agencies. OSTWG reported its findings about youth safety on the Internet to Congress on June 4, 2010.[14] Among its tasks, OSTWG reviewed and evaluated the status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, and age-appropriate labels for content. With respect to Internet safety education, OSTWG recommended greater interagency cooperation, publicity,

---

[14] *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group* (June 4, 2010), *available at* www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf.

and public-private sector cooperation for projects such as OnGuardOnline and *Net Cetera* to improve their national uptake in schools and local communities. As described above, the FTC is actively working to expand the reach of the already successful OnGuardOnline and *Net Cetera* projects.

IV. SOCIAL NETWORKING, MOBILE COMPUTING, AND P2P

In addition to education efforts to improve teen privacy, the Commission is also focused on specific technologies of which teens are particularly high users – social networking, mobile computing, and P2P file-sharing.

A. Social Networking

Social networking is pervasive among teens: 73 percent of American teens aged 12 to 17 now use social networking sites such as Facebook and MySpace, up from 55 percent two years ago.[15] Nearly half of teens use these sites on a daily basis to interact with their friends.[16] Teens use social networking to send messages to friends, post comments, and share photos and videos.[17]

The Commission has sought to protect teenage and other consumers in this environment through law enforcement, research, and education. It has brought a number of enforcement

---

[15] *See* Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), *available at* www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1.

[16] *See* Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), *available at* www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/More-details-from-the-survey.aspx?r=1..52

[17] *See* Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), *available at* www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

actions against social networking sites since 2006, when social networking exploded on the youth scene. Most recently, the Commission announced a consent order against Twitter, Inc. settling charges that it falsely represented to consumers that it would maintain reasonable security of its system and that it would take reasonable steps to ensure that private tweets remain private. Under the order, Twitter has agreed to maintain reasonable security and to obtain independent audits of its security procedures every two years for 10 years.[18] The Commission also has brought actions against several social networking sites that targeted youth but failed to adhere to the Children's Online Privacy Protection Act ("COPPA") with respect to users under the age of 13.[19] The Commission will continue to examine the practices of social networking sites and bring enforcement actions when appropriate.

In addition to its enforcement work, the Commission has been gathering information about social networking as part of a recently-concluded series of public roundtables on consumer privacy.[20] The goal of the roundtables was to explore how best to protect consumer privacy without curtailing technological innovation and beneficial uses of information.[21] Participants at

---

[18] *In re Twitter*, FTC File No. 092 3093 (June 24, 2010) (approved for public comment), *available at* www.ftc.gov/opa/2010/06/twitter.shtm.

[19] *United States v. Xanga.com, Inc.,* No. 06-CIV-6853(SHS) (S.D.N.Y.) (final order Sept. 11, 2006); *United States v. Industrious Kid, Inc.,* No. 08-CV-0639 (N.D. Cal.) (final order Mar. 6, 2008); *United States v. Sony BMG Music Entm't,* No. 08-CV-10730 (S.D.N.Y.) (final order Dec. 15, 2008); *United States v. Iconix Brand Group, Inc.*, No. 09-CV-8864 (S.D.N.Y.) (final order Nov. 5, 2009).

[20] More information about the Privacy Roundtables can be found at www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[21] Several key concepts emerged from the roundtable discussions. First, participants stated that data collection and use practices should be more transparent by, for example, simplifying privacy disclosures so that consumers can compare them. Second, participants said that it should be easier for consumers to exercise choice. For example, rather than burying

the roundtables repeatedly raised issues related to social networking, and a specific panel was devoted to the subject. Experts on this panel discussed the difficulty of defining consumer expectations on social networking sites, issues related to third-party applications that use data from social networking sites, and the effectiveness of privacy disclosures and privacy settings in the social networking space.

The Commission is reviewing the information it received as part of the roundtable series and drafting initial privacy proposals, which it will release for public comment later this year.[22] The Commission will consider the information it obtained about social networking as it makes its recommendations.

B. Mobile Technology

Teens' use of mobile devices is increasing rapidly – in 2004, 45 percent of teens aged 12 to 17 had a cell phone; by 2009, that figure jumped to 75 percent.[23] Many teens are using their phones not just for calling or texting, but increasingly for applications like emailing and web

---

important choices in a lengthy privacy policy, such choices should be presented at the most relevant time – e.g., the point of information collection or use. Further, it may not be necessary to provide choice about uses of data that are implicit or expected as part of a transaction – for example, sharing address information with a shipping company to send a product that the consumer has requested. Finally, participants noted that companies should build basic privacy protections into their systems at the outset by, for example, collecting and retaining information only if they have a business need to do so. The Commission is taking these basic principles into account as it develops privacy proposals to be released for comment later this year.

[22] In addition to the information presented at the roundtables, the Commission received over 100 submissions in response to its request for written comments or original research on privacy, *available at* www.ftc.gov/os/comments/privacyroundtable/index.shtm.

[23] Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), *available at* www.pewinternet.org/~/media//Files/Reports/2010/PIP-Teens-and-Mobile-2010.pdf.

browsing, including accessing social networking sites and making online purchases.[24] They are also using relatively new mobile applications that raise unique privacy concerns, such as location-based tracking.[25]

The FTC has been actively addressing privacy issues relating to mobile technology for several years. In 2008, the Commission held a Town Hall meeting to explore the evolving mobile marketplace and its implications for consumer protection policy. Participants in the meeting examined topics such as consumers' ability to control mobile applications and mobile commerce practices targeting children and teens. In April 2009, FTC staff issued a report setting out key findings and recommendations based on the Town Hall meeting. Having highlighted that the increasing use of smartphones presents unique privacy challenges regarding children, the Town Hall meeting led to an expedited regulatory review of the Children's Online Privacy Protection Rule.[26] The review is taking place this year, even though it was originally set for 2015.

More recently, the privacy roundtable discussions devoted a panel to addressing the privacy implications of mobile computing. This panel focused on two significant issues: the extent to which location-based services were proliferating in an environment without any basic rules or standards, and the degree to which transparency of information sharing practices is

---

[24] *Id.*

[25] Nielsen, *How Teens Use Media* (June 2009), *available at* blog.nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf.

[26] Under the rulemaking authority granted to it by the Children's Online Privacy Protection Act of 1998 ("COPPA"), the FTC promulgated the COPPA Rule, 16 C.F.R. Part 312, in 1999.

possible on mobile devices. As with social networking, the Commission staff's upcoming report on the privacy roundtables will further address these issues.

In addition to these policy initiatives, the FTC is ensuring that it has the tools necessary to respond to the growth of mobile commerce and conduct mobile-related investigations. In the past month, the FTC has expanded its Internet lab to include smartphone devices on various platforms and carriers. The Commission also has obtained the equipment necessary to collect and preserve evidence from these mobile devices. With these smartphones, FTC staff can now improve its monitoring of unfair and deceptive practices in the mobile marketplace, conduct research and investigations into a wide range of issues, and stay abreast of the issues affecting teens and all consumers.

C. P2P File-Sharing

P2P file-sharing allows people to share their files through an informal network of computers running the same software. Teens use P2P programs to share music, games, or software online. However, P2P file-sharing presents privacy and security risks because consumers may unknowingly allow others to copy private files they never intended to share. The FTC has sought to address these risks in several ways.

First, the Commission has undertaken an initiative targeting businesses that use or allow P2P programs on their networks without implementing reasonable safeguards to protect their customers' information from inadvertent disclosure through these programs. This customer information can be leaked onto a P2P network when, for example, an employee downloads a P2P program directly onto his or her work computer, or when a business chooses to utilize P2P file-sharing programs, but does not configure its network correctly to protect such information.

To address this problem, the Commission recently sent letters notifying several dozen public and private entities – including businesses, schools, and local governments – that customer information from their computers had been made available on P2P file-sharing networks.[27] In the notification letters, the FTC urged the entities to review their security practices, explained that they should take steps to control the use of P2P software on their networks, and shared new business education materials designed to help them protect their confidential data from inadvertent sharing to a P2P network.[28] Many entities that received these notifications contacted FTC staff for additional information to aid in their investigations into the file-sharing incidents, and a number reported making changes to their security practices to prevent inadvertent file-sharing to P2P networks. At the same time it sent the notification letters, the FTC opened non-public investigations into other companies whose customer or employee information had been exposed on P2P networks.[29]

FTC staff has also assisted P2P file-sharing software developers in devising best practices to help prevent consumers from inadvertently sharing personal or sensitive data over P2P networks. In July 2008, the Distributed Computer Industry Association published voluntary best practices to guard against inadvertent file sharing. With the assistance of an independent P2P technology expert, FTC staff have been assessing whether members are complying with these best practices.

---

[27] FTC Press Release, *Widespread Data Breaches Uncovered by FTC Probe*, (Feb. 22, 2010), *available at* www.ftc.gov/opa/2010/02/p2palert.shtm.

[28] These materials are available at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[29] FTC Press Release, *supra* note 27.

The FTC also seeks to educate consumers about the risks of P2P file sharing software. Among other things, the agency provides tips for consumers about P2P in a consumer alert entitled "P2P File-Sharing: Evaluate the Risks,"[30] which is available through OnGuardOnline.gov, and in *Net Cetera*.

Finally, the FTC has brought enforcement actions alleging that certain P2P file sharing software providers made deceptive claims in connection with the marketing of their products.[31]

V. PRIVACY MODELS AND TEENS

The issues surrounding teens' use of digital technology raise the question whether there should be special privacy protections for them. Some have suggested that COPPA's protections be extended to cover adolescents between the ages of 13 and 18; others suggest that separate privacy protections should be established for teens.[32]

---

[30] The consumer alert is available at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm.

[31] *FTC v. Cashier Myricks Jr.,* Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sep. 27, 2005) (suit against the operator of the web site MP3DownloadCity.com for making allegedly deceptive claims that it was "100% LEGAL" for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games); *FTC v. Odysseus Marketing, Inc.,* Civ. No. 05-330 (D.N.H., filed Sep. 21, 2005) (suit against website operator that encouraged consumers to download free software falsely marketed as allowing consumers to engage in anonymous P2P file-sharing).

[32] *See* Hearing: an Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection, Prepared Statement of Professor Kathryn Montgomery Before the Subcommittee on Consumer Protection, Product Safety, and Insurance, Committee on Commerce, Science, and Transportation, United States Senate (Apr. 29, 2010), *available at* www.democraticmedia.org/files/u1/2010-04-28-montgomerytestimony.pdf; *see also* An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA), Prepared Statement of Marc Rotenberg, EPIC.org, *available at* epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf.

The COPPA statute and implementing regulations enforced by the FTC require operators to provide notice to, and receive consent from, parents of children under age 13 prior to the collection, use, or disclosure of such children's personal information on web sites or online services. In the course of drafting COPPA, Congress looked closely at whether adolescents should be covered by the law, ultimately deciding to define a "child" as an individual under age 13. This decision was based in part on the view that most young children do not possess the level of knowledge or judgment to make appropriate determinations about when and if to divulge personal information over the Internet. The FTC supported this assessment.[33]

While this parental notice and consent model works fairly well for young children, the Commission is concerned that it may be less effective or appropriate for adolescents. COPPA relies on children providing operators with parental contact information at the outset to initiate the consent process. The COPPA model would be difficult to implement for teens, as they have greater access to the Internet outside of the home than young children do, such as in libraries, friends' houses, or mobile devices. Teens seeking to bypass the parental notification and consent requirements may also be less likely than young children to provide accurate information about their age or their parents' contact information. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly.[34] Moreover, given that teens are more likely than young

---

[33] *See* Testimony of the Federal Trade Commission Before the Subcommittee on Communications, Senate Committee on Commerce, Science & Transportation (Sept. 23, 1998), *available at* www.ftc.gov/os/1998/09/priva998.htm.

[34] *See*, *e.g.*, *American Amusement Mach. Ass'n. v. Kendrick*, 244 F.3d 572 (7th Cir. 2001) (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-14 (1975); *Tinker v. Des Moines Independent School District*, 393 U.S. 503, 511-14 (1969).

children to spend a greater proportion of their time online on websites that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.[35]

The Commission will continue to evaluate how best to protect teens in the digital environment and take appropriate steps to do so. In specific instances, there may be opportunities for law enforcement or advocacy in this area. For example, just this week, the Commission's Bureau of Consumer Protection sent a letter to individual stakeholders in XY corporation, which operated a now-defunct magazine and website directed to gay male youth. The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information – including names, street addresses, personal photos, and bank account information from gay teens. The letter warns that selling, transferring, or using this information would be inconsistent with the privacy promises made to the subscribers, and may violate the FTC Act; thus, the letter urges that the data be destroyed.

More generally, the FTC believes that its upcoming privacy recommendations based on its roundtable discussions will greatly benefit teens. The Commission expects that the privacy proposals emerging from this initiative will provide teens both a greater understanding of how their data is used and a greater ability to control such data. Finally, the Commission is available to work with this committee, if it determines to enact legislation mandating special protections for teens.

---

[35] *See ACLU v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (citing *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) ("Requiring users to go through an age verification process would lead to a distinct loss of personal privacy.")); *see also Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (citing *Butler v. Michigan*, 352 U.S. 380, 383 (1957) ("The Government may not reduce the adult population . . . to reading only what is fit for children.")).

VI. CONCLUSION

The Commission is committed to protecting all consumers in the digital environment, especially those consumers, such as teens, who are particularly vulnerable to threats on the Internet. The FTC will continue to act aggressively to protect teens through education, law enforcement, and policy initiatives that will better enable teens to control their information online.

Thank you for this opportunity to discuss the privacy and security of teens on the Internet. I look forward to your questions.