PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Pamela Jones Harbour, Commissioner
Federal Trade Commission

Before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

of the

COMMITTEE ON ENERGY AND COMMERCE

United States House of Representatives

Washington, D.C.

June 28, 2006

Mr. Chairman, Ranking Member Stupak, and members of the Subcommittee, I am Pamela Jones Harbour, a Commissioner at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to discuss the Commission's efforts to help ensure that parents and children understand the risks of social networking websites and the steps they can take to reduce these risks before participating on such sites.

I. Introduction

Technology constantly changes the ways that consumers can communicate with each other. The telephone was the primary technology consumers used to converse for most of the last century. During the 1980's and the 1990's, personal computers and the Internet vastly expanded the options available for consumers to communicate with each other – email, chat rooms, online bulletin boards, and instant messaging, to name a few. Social networking websites[2] are the next generation in communications technology, providing a platform for multi-faceted communication between participating users.

Children, especially teens and tweens,[3] have embraced this online technology. According to a 2005 report by the Pew Internet and American Life Project, 87% of children between the ages of 12 and 17 are online, and approximately 11 million of them access the

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any other individual Commissioner.

[2] Social networking sites host weblogs, or "blogs." A blog is a website where regular entries are made (such as in a journal or diary). Blogs often function as an online author's personal journal that also may contain hypertext, images, and links to video or audio files or other Web pages. *See* http://en.wikipedia.org/wiki/Blog.

[3] For purposes of this testimony, teens are children age 13 to 17, while tweens are children age 8 to 12.

Internet every day.[4] Teen use of social networking websites in particular has exploded recently. MySpace and Facebook reportedly rank among the top ten websites among children age 12 to 17, based on the average minutes they spent online.[5]

At the same time that social networking websites offer online communication, camaraderie, and community among teens and tweens, they, like other activities on the Internet, also can pose risks. Because the information that children post on their online journals, web logs or "blogs" can be accessed by other Internet users, social networking websites raise heightened privacy and security concerns. In particular, sexual predators may use the information that children provide on social networking sites to identify, contact, and exploit them,[6] unless these sites are constructed to reduce access to this information, or users themselves take steps to limit unwanted access.

The Federal Trade Commission is committed to helping create a safer online experience for children. I will discuss in more detail the agency's efforts to help protect children through consumer education and targeted law enforcement. In addition, I will discuss the need for social networking websites – individually, collectively, and, most importantly, expeditiously – to develop and implement safety features to protect children who visit their sites and empower

[4] *See* Pew Internet & American Life Project Report, *Teens and Technology: Youth Are Leading the Transition to a Fully Wired and Mobile Nation* (July 27, 2005), available at http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf.

[5] *See* comScore Media Metrix survey, *The Score: Teens Highly Engaged Online* (Mar. 16, 2006), available at http://www.imediaconnection.com/content/8691.asp.

[6] *See, e.g., Michigan Teen Home Safe & Sound: Authorities Say 16-Year-Old Flew To Mideast For 'MySpace' Rendezvous* (June 12, 2006), available at http://www.cbsnews.com/stories/2006/06/09/tech/main1697653.shtml; Tehani Schneider & Adam Teliercio, *Free Expression Blooms in Risk-laden MySpace*, Morristown Daily Record, May 14, 2006.

parents to protect their children when they do so.

II. Consumer Education

In response to the rapid increase in use of social networking sites by teens and tweens, one element of the FTC's "safe networking" program has been to develop user-friendly consumer education materials, both for parents and for children. Last month, the agency posted on our website two consumer publications providing practical guidance to parents, teens, and tweens about using social networking websites safely.

A. Advice for Parents

It is, of course, critically important for parents to know what their children are doing in cyberspace. Accordingly, one of the FTC's publications is directed specifically to parents, and describes in non-technical terms what social networking websites are, how they can pose risks to children, and how parents can monitor their children's activities on such sites.[7] The publication encourages parents to keep their home computers in an open area, such as the kitchen or family room, so that they can see where their children go when they go online.[8] Parents should use the Internet with their children, and visit popular sites, including social networking sites if their children are using them. Parents should review the information their children post on blog sites,[9]

[7] *See* FTC Facts for Consumers: Social Networking Sites: A Parents' Guide (May 2006), available at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.pdf.

[8] A March 2005 report by the Kaiser Family Foundation found that 31% of 8 to 18 year olds have a computer in their bedroom, and 20% have Internet access in their rooms. *See Generation M: Media in the Lives of 8-18 Year-olds* (Mar. 9, 2005), available at http://www.kff.org/entmedia/7251.cfm.

[9] According to a recent study, sixty-one percent (61%) of teens reveal their contact information on their blogs by disclosing their email address (44%), instant messenger name (44%), or a link to a personal home page (30%). Fifty-nine percent (59%) reveal their location in terms of a city or state. Thirty-nine percent (39%) of teen bloggers provide their birth date,

and encourage the use of privacy settings to restrict who can access and post on their children's sites.

B. Advice for Children

Another FTC publication is directed to teens and tweens, and gives them important safety tips if they are using social networking sites.[10] The brochure counsels them to think about how a particular social networking website works before they decide to join. For example, some sites allow only access by a defined community of users. Others allow anyone and everyone to view their postings. If teens and tweens decide to join a particular social networking website, they should consider using the site's particular privacy settings to limit access to their postings.

Moreover, the publication warns teens and tweens to be cautious about the information they post. They should post neither information that can be used to locate them in the offline world (for example, they should not post their full name, address, phone number), nor information that could be used to facilitate identity theft. The agency also warns them that school admissions officers and potential employers may be able to look at their photos and postings. Finally, it warns that once information is posted online, it may be impossible to take it back. Even if the teen or tween deletes the information from his or her own site, older versions may still exist on other people's computers. Above all, children must know that engaging in risky behavior online (such as "flirting" with someone they do not know offline) can have

and twenty percent (20%) disclose their full name. *See* David Huffaker, *Teen Blogs Exposed: The Private Lives of Teens Made Public* (2006), available at http://www.soc.northwestern.edu/gradstudents/huffaker/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf.

[10] *See* FTC Facts for Consumers: Social Networking Sites: Safety Tips for Teens and Tweens (May 2006), available at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.pdf.

serious, even deadly, consequences, and they should be wary about meeting in person someone whom they know only from the online world.

C. OnGuardOnline

The FTC's consumer information on social networking websites also is featured prominently on OnGuardOnline.gov, an innovative multimedia website designed to educate consumers about basic computer security practices. OnGuardOnline has become the hallmark of the Commission's larger cybersecurity campaign. OnGuardOnline is built around seven timeless tips about online safety.[11] In addition, the site hosts specific information modules on topics such as social networking, wireless security, identity theft, phishing, spyware, and spam. OnGuardOnline features up-to-date articles from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), such as a newly added piece on the troubling practice of "Cyberbullying," that is, using technology to harass, or bully, someone else. There also is a video for parents on "Teaching Kids Online Safety."

In the past two months, OnGuardOnLine has had between six and seven thousand unique visitors each day. In early June 2006, the FTC's social networking tips for parents and tips for teens and tweens were, respectively, the second and third most popular pages on OnGuardOnline, after the site's home page. Comcast.net recently promoted the social

[11] *See* http://www.OnGuardOnline.gov. The seven tips are described in detail in the FTC publication, Stop Think Click: Seven Practices for Safer Computing, available at http://onguardonline.gov/stopthinkclick.html. The seven practices for safer computing are: (1) Protect your personal information; (2) Know who you're dealing with; (3) Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly; (4) Be sure to set up your operating system and Web browser software properly, and update them regularly; (5) Protect your passwords; (6) Back up important files; and (7) Learn who to contact if something goes wrong online.

networking module as a "featured link," driving significant traffic to the website, and Verizon DSL's customer default homepage and TRUSTe link directly to the social networking module, as well.

OnGuardOnline was developed through a partnership with cybersecurity experts, consumer advocates, online marketers, and other federal agencies. It is a great example of public-private cooperation. The agency deliberately branded OnGuardOnline independently of the Federal Trade Commission to encourage other organizations to make the information their own and to disseminate it in ways that reach the most consumers.

Many of the social networking websites themselves have linked directly to the social networking module on OnGuardOnline. Thus far, eleven of the social networking websites most popular with teens either have already posted links to FTC materials or have informed our staff that they will do so in the near future,[12] and these links have directly contributed to the increased traffic at OnGuardOnline.

III. Law Enforcement

Congress enacted the Children's Online Privacy Protection Act – or COPPA – to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet.[13] The statute gives

[12] The sites that have posted links to OnGuardOnline include: Alloy (http://www.sconex.com/content/safety.php); Buzznet (http://www.buzznet.com); Facebook (http://www.facebook.com/help.php?tab=abuse); Friendsorenemies (http://www.friendsorenemies.com/about.php); MyYearbook (http://www.myyearbook.com); TagWorld (http://tagworld.com/-/Main.aspx).; and Yahoo! 360° (http://security.yahoo.com). The sites that have informed FTC staff that they will post the materials are: HI5; Microsoft Spaces; MySpace; and Tagged.

[13] *See* Statement of Basis and Purpose, 16 C.F.R. Part 312.

parents the power to determine whether and what information is collected online from their children under age 13, and how such information may be used. COPPA, and its implementing rules, apply to operators of websites directed to children under the age of 13.[14] They also apply to operators of general audience websites who have actual knowledge that they are collecting personal information from children under the age of 13, which includes some social networking websites.[15]

COPPA and its implementing Rule mandate that website operators take several affirmative steps *before* collecting, using, or disclosing personal information from a child under age 13. They must post on their websites a copy of their privacy policy. Operators also must provide parents with a notice describing their privacy policies. They must obtain verifiable consent from a parent or guardian before collecting personal information from children. And once operators have collected this information, they must establish and maintain reasonable procedures to protect its confidentiality, security, and integrity.[16]

The FTC staff currently is investigating several social networking websites to determine

[14] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6508, and the Commission's COPPA Rule, 16 C.F.R. Part 312.

[15] The Commission has brought two cases in which website operators were alleged to have had actual knowledge that they were collecting personal information from children under 13 on their general audience websites. *See United States v. UMG Recordings, Inc.*, Civ. No. CV-04-1050 JFW (Ex) (C.D. Cal. Feb. 17, 2004) (civil penalty of $400,000); *United States v. Bonzi Software, Inc.,* Civ. No. CV-04-1048 RJK (Ex) (C.D. Cal. Feb. 17, 2004) (civil penalty of $75,000). Neither of these cases involved social networking sites.

[16] The COPPA Rule also empowers parents to protect their children under 13 even after consenting to a website operator's collecting information from them. If and when parents ask, site operators must provide them with the means to review the personal information that has been collected from their children. A site also must give parents the opportunity to prevent further collection or use of that information, as well as the chance to delete the information.

whether they are in compliance with COPPA and its implementing Rule.

IV. Looking Ahead: Self-Regulation and Industry Best Practices

Consumers, government, technology companies, and advertisers all have a shared interest and responsibility in creating a secure online environment. Social networking website operators are no exception.

The social networking industry has a clear incentive to create a safe online community. They owe this to their users, and sites that do not make online safety a priority may find it hard to compete with those that do. Some social networking websites already allow users to restrict access to the information they post, such as by creating sites with more closed, defined communities or enhancing specific privacy features on their sites.

Last week, two summits addressed issues posed by social networking sites, one hosted by the National Center for Missing and Exploited Children and the other hosted by WiredSafety.org. These summits focused, in part, on industry best practices. These meetings are positive steps to encouraging a meaningful industry response to the risks that social networking sites pose for children. The Commission hopes that the momentum from these summits continues to build so that industry best practices are developed and implemented as quickly as possible.

V. Conclusion

The Commission has been at the forefront of efforts to safeguard children’s information online and to educate consumers about the risks involved in social networking. The agency is committed to continuing this important work. The FTC also is committed to working with this Subcommittee to provide greater security and privacy for American consumers.