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

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 m

d 0 l8 Tc lle Tme l8 TRT-5.04 Tm(children provide on soci42.0249-31 ac(T)lETess 2 9- 000t16 6 0 and es348.0248-31 ac(The Federal Trade Com)l8 T12 4dis. seh20 16d

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, 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 inform 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] *.2072186.8457.680P3nd asative m*

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.m

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.

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.