But we are here today because our children's online interactions in the Web 2.0 world are not all fun and games. Seven percent of online teens say they have been contacted by a stranger – either through "friend" requests, spam email, or comments posted on a blogging or photo sharing site – who made them feel scared or uncomfortable.[4] Reports of online cyberbullying also are on the rise – according to recent research, nearly 1 in 3 children ages 10 to 17 actually reported having harassed someone online at least once in the past year.[5] As a society, our concerns about protecting children online do not end with their exposure to uncomfortable contacts and nasty messages. We also are worried about children's ability to view inappropriate material online, and, in the worst instances, that their images are being shared worldwide through a nefarious net of child pornographers.

Even where children's online safety is not at risk, their privacy may be. Children are being asked to reveal, or are voluntarily divulging, a great deal more personal information about themselves and their families than may be advisable. Finally, as children's use of the Internet continues to rise, so does their potential exposure to spyware, identity theft, and phishing scams.

Today, we will roll up our sleeves and talk about what more we, as government representatives, technology companies, researchers, and website operators, can do to protect children in this online world. For our part, the Federal Trade Commission is deeply committed to doing what it can to protect children's privacy and security online. Yet, as responsible government officials, we also respect the First Amendment's protection of free speech. The

---

[4]Pew Internet & American Life Project, "Teens and Online Stranger Contact" (Oct. 14, 2007).

[5]Ybarra M., Mitchell K., *Prevalence and frequency of Internet harassment instigation: Implications for adolescent health*, J. ADOLESCENT HEALTH 41, 189–195 (2007).

government is necessarily limited in when, and how, it can step in to protect children from inappropriate material. Limited, but not powe

[6]15 U.S.C. §§ 41-58, *as amended.*

[7]*FTC v. Various, Inc. d/b/a AdultFriendFinder,* No. 5:07-cv-6181 (N.D. Cal. filed Dec. 6, 2007), *available at* http://www.ftc.gov/opa/2007/12/afriendfinder.shtm

defendant from disseminating sexually explicit advertisements to consumers who are not seeking out sexually explicit material; it also requires the defendant to monitor its marketing affiliates and other third parties involved in advertising its sexually explicit websites.[8]

In addition to our general authority to challenge deceptive and unfair practices, in 2003, Congress gave the FTC and the Department of Justice specific authority to tackle the problem of sexually explicit email communications. The CAN-SPAM Act,[9] and the FTC's Adult Labeling Rule,[10] strive to place a bumper between "X-rated" email and children. Commercial e-mailers must alert recipients to the presence of sexually explicit content in the subject line, and must make sure that the initially viewable area of the email message contains no graphic sexual images. We have brought 10 cases involving the Adult Labeling Rule, garnering over $1.6 million in civil penalties, and over $900,000 more in disgorgement of ill-gotten gains.[11]

---

[8] *Id. See also FTC v. Zuccarini*, No. 01-CV-4854 (E.D. Pa. filed Oct. 1, 2001), *available at* http://www.ftc.gov/os/caselist/0123095/index.shtm (alleging unfairness and deception against a defendant who registered various misspellings of a children's cartoon site and a pop star to redirect users to sites showing pornographic images); *FTC v. Pereira*, No. 99-1367-A (E.D. Va. filed Apr. 14, 1999), *available at* http://www.ftc.gov/os/caselist/9923264/990922comp9923264.shtm (case alleging deception and unfairness against defendants who "hijacked" certain web pages and forced consumers who had searched for non-sexually explicit topics to be taken to adult websites).

[9] 15 U.S.C. §§ 7701-7713.

[10] 16 C.F.R. Part 316.4.

[11] *U.S. v. TJ Web Productions, LLC,* Civil Action No: CV-S-05-0882-RLH-GWF (D. Nev. filed Dec. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523047/0523047.shtm ($465,000 civil penalty); *FTC v. Cleverlink Trading Ltd.*, Case No. 05C 2889 (N.D. Ill. filed Jul. 25, 2006), *available at* http://www.ftc.gov/os/caselist/0423219/0423219.shtm ($400,000 disgorgement of ill-gotten gains); *FTC v. William Dugger*, Civil Action No. CV06-0078-PHX-ROS (D. Ariz. filed Jan. 10, 2006), *available at* http://www.ftc.gov/os/caselist/0523161/0523161.shtm ($8,000 disgorgement of ill-gotten gains); *FTC v. Global Net Solutions, Inc.*, Civil Action No. CV-S-05-0002-PMP-LRL (D. Nev. filed August 4, 2005), *available at* http://www.ftc.gov/os/caselist/0423168/0423168.shtm ($621,000

disgorgement of ill-gotten gains); *U.S. v. APC Entertainment, Inc.*, FTC File No. 052-3043 (S.D. Fla. filed July 20, 2005), *available at* http://www.ftc.gov/os/caselist/0523043/0523043.shtm ($220,000 civil penalty); *U.S. v. BangBros,com, Inc.*, FTC File No. 042-3180 (S.D. Fla. filed Jul. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423180/0423180.shtm ($650,000 civil penalty); *U.S. v. Cyberheat, Inc.*, FTC File No. 052-3042 (D. Ariz. filed Jul. 20, 2005) (litigation pending); *U.S. v. Impulse Media Group, Inc.*, FTC File No. 052-3046 (W.D. Wa. filed Jul. 20, 2005) (litigation pending); *U.S. v. MD Media, Inc.*, FTC File No. 052-3044 (E.D. Mich. filed Jul. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0523044/0523044.shtm ($238,743 civil penalty); *U.S. v. Pure Marketing Solutions, LLC*, FTC File No. 052-3045 (M.D. Fla. filed Jul. 20, 2005, *available at* http://www.ftc.gov/os/caselist/0523045/0523045.shtm ($50,000 civil penalty).

See

47 U.S.C. § 231.

United States Postal Inspection Service, the Department of Commerce, Technology Administration, the Internet Education Foundation, the National Cyber Security Alliance, i-SAFE, AARP, the Direct Marketing Association, the National Consumers League, the Better Business Bureaus, and others.

OnGuardOnline.gov is popular; it has logged more than 4 million unique visitors in its first two years. It currently attracts 200,000-300,000 unique visits each month. OnGuard Online is branded independently of the FTC, so other organizations can make the site and the information their own. The FTC encourages companies and other organizations to help fight Internet fraud, scams, and identity theft by sharing the tips at OnGuardOnline.gov with their employees, customers, members and constituents. OnGuard Online materials also are available in Spanish, at AlertaenLinea.gov.

Many topics presented on OnGuardOnline apply to consumers generally. In certain areas, however, we have focused on the issues uniquely important to children and their parents. OnGuardOnline includes a video for parents on how to weigh the risks of children's online activities, and provides some thoughtful guidelines for kids' Internet use. With the rise in popularity of social networking sites, last year, we introduced a set of tips about safer social networking. One bulletin is for parents, and one is specifically directed to teens, using different language for each audience. The site also includes an interactive "Buddy Builder" quiz aimed at getting teens to consider whom they "friend" online. Since its introduction, the social networking page has been the single most visited page on OnGuardOnline.

Our OnGuardOnline materials are not static; they change as technological developments change. For example, after noting the reality that increasing numbers of children now access the Internet not from stand-alone PCs, but from their mobile handsets, in September we updated our

social networking tips for parents alerting them to possible limits that they can place on a child's cell phone.[17] We will continuously update our educational materials to take into account developments in children's use of the Internet and technology, and will shortly add a section on filtering techniques and other tools that parents might employ to keep younger children from viewing inappropriate materials.

Representative Bean's "SAFER NET Act" directs the FTC to implement a national education campaign on Internet safety, including children's Internet safety, and to authorize funding for such a campaign.[18] We greatly appreciate the recognition this bill provides for our existing computer education initiatives, including OnGuardOnline. In addition, because the SAFER Net Act refers to several child safety areas that constitute criminal activity beyond the FTC's authority, we are planning to partner with the government agencies active in protecting children from cyber-crimes and with prominent non-governmental organizations, to expand the scope of topics beyond those currently covered by OnGuard Online.[19] The result should be an even stronger site that serves as an umbrella for all of the federal government's Internet safety information.

---

[17]*See* http://onguardonline.gov/socialnetworking.html ("Social Networking: A Parent's Guide," September 2007).

[18]H.R. 3461, 110th Cong. (2007).

[19]*See* Prepared Statement of the Federal Trade Commission, "Enhancing FTC Consumer Protection in Financial Dealings, with Telemarketers, and on the Internet," before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce of the United States House of Representatives, presented by Lydia B. Parnes, Director, Bureau of Consumer Protection (October 23, 2007), *available at* http://www.ftc.gov/os/testimony/071023ReDoNotCallRuleEnforcementHouseP034412.pdf.

mechanisms for reporting abuse, guidelines for strong privacy settings, record-keeping requirements so that sites can follow patterns of abuse, increased levels of human oversight, and better cooperation with criminal authorities, especially among the smaller sites. There also should be an enforcement mechanism in place so that the failure to adhere to these guidelines is followed by oversight and corrective action.

I have long expressed the belief that effective industry self-regulation can have significant benefits, and can, in specific instances, address problems more quickly, creatively, and flexibly than government regulation. This approach has proven extremely successful in the past, in many areas, especially where the government's jurisdiction to handle particular matters may, like here, be constrained by constitutional principles.

In our experience, the best self-regulatory programs have clear guiding principles: they clearly address the problems they seek to remedy; they are flexible and able to adapt to new developments within the industry; they are enforced and widely followed by affected industry members; they are visible and accessible to the public; they are independent from their member firms; and they objectively measure member performance and impose sanctions for noncompliance.

There are a number of examples of effective self-regulatory programs that fit these criteria. The Better Business Bureau's self-regulatory oversight of national advertising[22] is one example. The BBB operates a National Advertising Division, typically referred to as NAD.

---

[22]The Council of Better Business Bureaus runs a number of advertising self-regulatory programs: the National Advertising Division (*see* http://www.nadreview.org/); the Children's Advertising Review Unit (see www.caru.org); the Electronic Retailing Self-Regulation Program (*see* www.narcpartners.org/ersp/); and the Children's Food and Beverage Advertising Initiative (*see* www.cbbb.org/initiative/).

See “Policies and Procedures by The National Advertising Review Council, Part 3.1,

[25]Prepared Statement of the Federal Trade Commission On Social Networking Sites, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce of the United States House of Representatives, presented by Commissioner Pamela Jones Harbour (June 28, 2006), *available at*