Federal Trade Commission

"Rights and Responsibility: Protecting Children in a Web 2.0 World"
Family Online Safety Institute
December 6, 2007

Keynote Address by Chairman Deborah Platt Majoras

Good morning. I am pleased to be here together with so many of our partners in safety – Commissioner Tate of the FCC, representatives of our international counterpart agencies, researchers, educators, corporate representatives, and the Family Online Safety Institute and other policy stakeholders.

Virtually no one disputes that the Internet holds great promise for us, and for our children, who have embraced this ever-evolving technology with enthusiasm. A full 93 percent of children ages 12-17 are online![1] Over half of online teens have created profiles on social networking and blogging sites.[2] And 89 percent of online teens say the Internet, and other electronic devices such as cell phones, MP3 players, and digital cameras, make their lives easier.[3]

---

[1]Pew Internet & American Life Project, "Parent and Teenager Internet Use" (Oct. 24, 2007).

[2]Pew Internet & American Life Project, "Teens, Privacy & Online Social Networks" (Apr. 18, 2007).

[3]Pew Internet & American Life Project, "Parent and Teenager Internet Use" (Oct. 24, 2007).

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 powerless.

Today, I will highlight some of the FTC's recent law enforcement activities to protect children online. I will then discuss the need to educate children and their parents about how to stay safe online. Finally, I will talk about the importance of meaningful industry self-regulation in this area.

I. The FTC's Law Enforcement Efforts

Making the Internet more secure is a central focus of the FTC's civil law enforcement mission. To that end, we have used our general statutory mandate under the Federal Trade Commission Act to protect the rights of consumers, including children, to avoid unwanted and potentially offensive content online.[6] We also have several specific statutory tools at our disposal that target what children see in emails and what they share on websites.

Using our general unfairness authority under the Federal Trade Commission Act to address the unwanted online intrusion of sexually explicit material, today we announce a settlement with the operators of AdultFriendFinder.com, touted as "the world's largest sex and swingers personals community."[7] Unfortunately, AdultFriendFinder did not keep its ads confined to the sex and swingers community. Rather, to lure consumers to its sites, the operator used spyware and adware to deliver pop-up ads containing graphic, sexually explicit images. These images often were foisted on consumers, including minors, who were not visiting sexually-oriented websites but rather were generally surfing the web. Our order bars the

---

[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

Finally, in an effort to address not only what children are exposed to online, but also what they post online, the FTC has actively enforced the Children's Online Privacy Protection Act, or what is affectionately known as COPPA ("kah-puh").[12] COPPA is the only child-specific federal privacy law in the United States, and it prohibits asking, or allowing, young children to provide personal information to a website operator without their parents' prior, verified, consent. If a child happens to provide personal information to a site without a parent's permission, COPPA grants parents the absolute right to contact the site and have the child's personal information removed.

Thus far, we have filed eleven COPPA civil penalty actions and obtained almost $2 million in penalties.[13] Our case last year against the social networking website Xanga.com,

---

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).

[12]*See* Privacy Online: A Report to Congress (June 1998), *available at* http://www.ftc.gov/reports/privacy3/toc.shtm.

[13]*U.S. v. Xanga.com, Inc.*, Civil Action No. 06-CIV-6853(SHS) (S.D.N.Y. filed Sept. 7, 2006), *available at* http://www.ftc.gov/opa/2006/09/xanga.shtm ($1 million civil penalty); *U.S. v. UMG Recordings, Inc.*, Civil Action No. CV-04-1050 (C.D. Cal. filed Feb. 18, 2004), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm ($400,000 civil penalty); *U.S. v. Bonzi Software, Inc.*, Civil Action No. CV-04-1048 (C.D. Cal. filed Feb. 18. 2004), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm ($75,000 civil penalty); *U.S. v. Mrs. Fields Famous Brands, Inc.,* Civil Action No. 2:03 CV205 JTG (D. Utah filed Feb. 27, 2003), *available at* http://www.ftc.gov/opa/2003/02/hersheyfield.shtm ($100,000 civil penalty); *U.S. v. Hershey Foods Corp.*, Civil Action No. 4:CV03-350 (M.D. Pa. filed Feb. 27, 2003), *available at*

which knowingly collected personal information from, and created blog pages for, 1.7 million users indicating they were kids, without their parents' permission, contained a record $1 million in civil penalties.[14]

The Xanga case cuts to the core of COPPA's goals – parents want to be informed, in advance, before their young children divulge their personal information. This is especially true in the Web 2.0 world where, with the mere click of a mouse, a child's personal information can be shared with the entire world. Parents also want the ability to say "no" to their children's online participation. In fact, many parents who ultimately discovered that their very young kids had created Xanga pages were quite upset, and a part of our case was based on the fact that Xanga, through customer service failures, did not provide parents with the opportunity to review or have deleted their children's personal information. I assure you that more COPPA cases are on their way.

II. Education

As you know, the government does not have an unfettered ability to protect children from viewing harmful material. In 1998, Congress passed the Children's Online Protection Act, or

---

http://www.ftc.gov/opa/2003/02/hersheyfield.shtm ($85,000 civil penalty); *U.S. v. The Ohio Art Company*, Civil Action No. 02-CV-7203 (N.D. Ohio filed Apr. 22, 2002), *available at* http://www.ftc.gov/opa/2002/04/coppaanniv.shtm ($35,000 civil penalty); *U.S. v. American Popcorn Co.*, Civil Action No. 02-CV-4008 (N.D. Iowa filed Feb.14, 2002), *available at* http://www.ftc.gov/opa/2002/02/popcorn.shtm ($10,000 civil penalty); *U.S. v. Lisa Frank, Inc.*, Civil Action No. 01-1516-A (E.D. Va. filed Oct. 3, 2001), *available at* http://www.ftc.gov/opa/2001/10/lisafrank.shtm ($30,000 civil penalty); *U.S. v. Monarch Services, Inc.*, Civil Action No. AMD 01 CV 1165 (D. Md. filed Apr. 21, 2001) ($35,000 civil penalty); *U.S. v. Bigmailbox.com, Inc.*, Civil Action No. 01-606-B (E.D. Va., filed Apr. 21, 2001) ($35,000 civil penalty); *U.S. v. Looksmart Ltd.*, Civil Action No. 01-605-A (E.D. Va. filed Apr. 21, 2001), *available at* http://www.ftc.gov/opa/2001/04/girlslife.shtm ($35,000 civil penalty).

[14] *U.S. v. Xanga.com, Inc., supra* note 13.

COPA ("koh-puh") – not to be confused with COPPA – which gave the Department of Justice the authority to prosecute criminally the knowing exposure of children online to material deemed harmful to minors.[15] The day after the law was signed, the ACLU and other plaintiffs filed suit, challenging the statute on First and Fifth Amendment grounds.[16] The law has had a tortured procedural history, and has never gone into effect. COPA serves as a stark reminder that it may be impossible to define with precision what constitutes content harmful to minors and to limit their exposure to it in a way that does not also unduly impinge on the First Amendment rights of adults.

Thus, enacting new laws is not the only answer. One of the most promising ways to help children stay safe online is to empower parents and their children through effective education.

At the FTC, we are actively engaged in a comprehensive education campaign to instill the values of safer and more secure computing. The cornerstone of our campaign is the multimedia website, OnGuardOnline.gov. We created the site in September 2005, partnering with other federal agencies, consumer advocates, and the technology industry to help computer users guard against Internet fraud, secure their systems, and protect their personal information. Among other topics, the site includes materials on spam, spyware, P2P file-sharing, phishing, identity theft, and wireless security. The FTC maintains OnGuardOnline.gov with significant content and marketing assistance from partners including: the U.S. Department of Justice, the

---

[15] 47 U.S.C. § 231.

[16] *See ACLU v. Reno,* 31 F. Supp. 2d, 473 (E.D. Pa. 1999). The case currently is on appeal to the 3rd Circuit Court of Appeals. For a description of the extensive procedural history of the case, see the government's appeal brief in *ACLU v. Alberto R. Gonzales,* Civil Action No. 07-2539 (3rd Cir. filed Sept. 17, 2007), *available at* http://www.aclu.org/pdfs/freespeech/copa_gov_appeal.pdf.

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.

III. Self-Regulation

Self regulation is another key component in protecting children online. This afternoon, you will hear from a set of panelists debating whether "companies or governments should do the most to protect children online." The answer, in my mind, is "yes, and yes." We, as the government, will do all that we are able to do. Companies can, and must, do the same.

This is an area ripe for technological innovation. As the Supreme Court recognized in considering the COPA case, widespread mechanisms that give parents the ability to screen, filter, and even monitor their children's online activities already exist.[20] FOSI has played a key role in facilitating labeling that works with parental control filters, and companies are free to voluntarily label or rate their content in a way that the government likely could never require them to do.

However, the efforts to protect children from online threats cannot stop with the voluntary labeling of companies' websites. Today's Internet is simply too vast, and the content in many cases comes not from companies but from users themselves. Moreover, in a recent survey, only 41 percent of parents indicated that they used parental controls to block their children's access to certain websites.[21]

The "Web 2.0" world would benefit from private sector initiatives, and it is here that technology companies and website operators should focus their attention. Parental controls, ratings and filtering technologies are important but not sufficient. Another key piece is the development of credible and effective self-regulatory programs. Such a program might call for

---

[20] *See Ashcroft v. ACLU,* 535 U.S. 564 (2002).

[21] *See* The Kaiser Family Foundation, "Parents, Children & Media," (June 2007), *available at* http://www.kff.org/entmedia/upload/7638.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/).

NAD gathers complaints about advertising. In investigating challenges to a particular company's advertising, the NAD enforces FTC-like standards for truth and accuracy in advertising. Most NAD inquiries are resolved at this level; if, however, the advertiser is not satisfied with the NAD's decision, the matter may be appealed to the National Advertising Review Board, or NARB.[23] Then, if the advertiser refuses to comply with the decision of NAD or of the NARB, the matter may be referred to the FTC for resolution.[24] This self-regulatory program of graduated enforcement is working well. Since 2004, we have received 44 NAD referrals, and followed up with appropriate enforcement action. We have told industry groups that ignoring the NAD process will enhance the risk of FTC review – something few companies want – and hope that this will foster utilization of the self-regulatory process before it reaches our level.

Other models include the self-regulatory rating systems of the movie and video game industries. Many people may not realize that these systems are strictly voluntary and are not required by law. As we have reported in our numerous reports on media violence, these systems generally have been responsive and flexible enough to evolve over the years to respond to new developments and concerns regarding electronic games and movies.

On the vast World Wide Web, there is no comparable comprehensive self-regulatory system. Indeed, even in the specific area of social networking sites, there has been no overarching development of guiding principles or a system of oversight.

---

[23] *See* "Policies and Procedures by The National Advertising Review Council, Part 3.1, *available at* http://www.nadreview.org/Procedures.asp?SessionID=.

[24] *Id.* at Part. 3.7.

In June 2006, the FTC called on representatives of the social networking industry to develop and implement safety guidelines.[25] Several of the social networking sites stepped up to the plate, and now provide users with a wide spectrum of privacy controls that allow a more nuanced approach to the "friends" phenomenon. In addition, several sites have established more responsive abuse reporting mechanisms, and are publicizing these mechanisms more widely, so that children who feel threatened or concerned have a reporting tool at their immediate disposal. We are also pleased that several social networking sites have linked to our OnGuardOnline tips for staying safe on social networking sites.

However, on social networking sites, and across the World Wide Web, the effort to provide meaningful privacy settings and responsive customer service still remains site-specific and reactive, often in response to government action or negative press attention. Website operators, can, and should, be more proactive in articulating a set of best practices and taking swift action, when problems arise. The incentives to create a safer online community should be clear. Operators 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.

Conclusion

No one organization, public or private, can adequately give parents the help they need in protecting their children on-line. Let us renew our commitment to working together to make improvements so that we can meet the twin goals of protecting children online, while at the same time ensuring that they can continue to enjoy the benefits of this information age.

Thank you.

---

[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* www.ftc.gov/os/2006/06/060626socialnetworking.pdf.