PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

CONSUMER PRIVACY AND PROTECTION IN THE MOBILE MARKETPLACE

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

May 19, 2011

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am David C. Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on consumer protection issues in the mobile marketplace.[1]

This testimony first highlights the expansive growth of the mobile arena and what it means for U.S. consumers. Second, it summarizes the Commission's response to new mobile technologies, the Commission's expansion of its technical expertise, recent law enforcement actions in the mobile arena (adding to the Commission's extensive law enforcement experience in areas relating to the Internet and privacy),[2] and its examination of consumer privacy issues raised by mobile technologies. Third, it discusses the application of a Do Not Track mechanism in the mobile environment.[3] And finally, the testimony discusses the special issues that mobile technologies raise for the privacy of children and teens, and provides an update of the Commission's review of the Children's Online Privacy Protection Rule.

I. The Mobile Marketplace

Mobile technology is exploding with a range of new products and services, and

---

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

[2] In the last fifteen years, the FTC has brought more than 30 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA"); 96 spam cases; 15 spyware cases; and 16 cases against companies for violating the Children's Online Privacy Protection Act.

[3] Commissioner William E. Kovacic dissents from this testimony to the extent that it endorses a Do Not Track mechanism. He believes that the endorsement of a Do Not Track mechanism is premature.

consumers across the country are rapidly responding to the industry's creation of smarter devices. According to the wireless telecommunications trade association, CTIA, the wireless penetration rate reached 96 percent in the United States by the end of last year.[4] Also by that same time, 27 percent of U.S. mobile subscribers owned a smartphone,[5] which is a wireless phone with more powerful computing abilities and connectivity than a simple cell phone. Such mobile devices are essentially handheld computers that offer web browsing, e-mail, and a broad range of data services. These new mobile devices allow consumers to handle a multitude of tasks in the palms of their hands and offer Internet access virtually anywhere.

Companies are increasingly using this new mobile medium to provide enhanced benefits to consumers, whether to provide online services or content, or to market other goods or services.[6] For example, consumers can search web sites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. They can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase or download mobile software applications ("apps") that can perform a range of consumer services such as locating the nearest retail stores, managing

---

[4] CTIA, *Wireless Quick Facts*, *available at* www.ctia.org/advocacy/research/index.cfm/aid/10323.

[5] ComScore, *The 2010 Mobile Year in Review Report* (Feb. 14. 2011), at 5, *available at* www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Mobile_Year_in_Review.

[6] Indeed, a recent industry survey found that 62 percent of marketers used some form of mobile marketing for their brands in 2010 and an additional 26 percent reported their intention to begin doing so in 2011. *See* Association of National Advertisers, Press Release, *Vast Majority of Marketers Will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011*, (Jan. 31, 2011) (describing the results of a survey conducted by the Association of National Advertisers and the Mobile Marketing Association), *available at* www.ana.net/content/show/id/20953.

shopping lists, tracking family budgets, transferring money between accounts, or calculating tips or debts.[7] Apps also allow consumers to read news articles, play interactive games, and connect with family and friends via social networks. Any of these services can contain advertising, including targeted advertising.

II. FTC's Response to Consumer Protection Issues Involving Mobile Technology

New technology can bring tremendous benefits to consumers, but it also can present new concerns and provide a platform for old frauds to resurface. Mobile technology is no different, and the Commission is making a concerted effort to ensure that it has the necessary technical expertise, understanding of the marketplace, and tools needed to monitor, investigate, and prosecute deceptive and unfair practices in the mobile arena.

A. Developing an Understanding of Mobile Issues Through Workshops and Town Halls

For more than a decade, the Commission has explored mobile and wireless issues, starting in 2000 when the agency hosted a two-day workshop studying emerging wireless Internet and data technologies and the privacy, security, and consumer protection issues they raise.[8] In 2006, the Commission held a three-day technology forum that prominently featured

---

[7] Although Apple's App Store and Google's Android Market are less than three years old, they collectively contain more than 600,000 apps. In January 2011, Apple reported that ten billion apps had been downloaded from the App Store. In May 2011, Google announced that 4.5 billion apps had been downloaded from the Android Market. *See* www.apple.com/itunes/10-billion-app-countdown/; googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html.

[8] FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, *available at* www.ftc.gov/bcp/workshops/wireless/index.shtml.

mobile issues.[9] Shortly thereafter, the Commission hosted two Town Hall meetings to explore the use of radio frequency identification (RFID) technology, and its integration into mobile devices as a contactless payment system.[10] And in 2008, the Commission held a two-day forum examining consumer protection issues in the mobile sphere, including issues relating to ringtones, games, chat services, mobile coupons, and location-based services.[11]

Most recently, as discussed below, the Commission examined the privacy issues raised by mobile technologies as part of a series of roundtables on consumer privacy in late 2009 and early 2010.

B. Developing a Mobile Lab and Creating a Mobile Team

The FTC has hired technologists (including its first Chief Technologist) and invested in new technologies to enable its investigators and attorneys to respond to the growth of mobile commerce and to conduct mobile-related investigations.[12] For many years, FTC Bureau of Consumer Protection staff have investigated online fraud using the agency's Internet Lab, a facility that contains computers with IP addresses not assigned to the government, as well as evidence-capturing software. The agency has expanded the Internet lab to include mobile

---

[9] FTC Workshop, *Protecting Consumers in the Next Tech-ade*, *available at* www.ftc.gov/bcp/workshops/techade. The Staff Report is available at www.ftc.gov/os/2008/03/P064101tech.pdf.

[10] FTC Workshop, *Pay on the Go: Consumers and Contactless Payment*, *available at* www.ftc.gov/bcp/workshops/payonthego/index.shtml; FTC Workshop, *Transatlantic RFID Workshop on Consumer Privacy and Data Security*, *available at* www.ftc.gov/bcp/workshops/transatlantic/index.shtml.

[11] FTC Workshop, *Beyond Voice: Mapping the Mobile Marketplace, available at* www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

[12] *See, e.g.*, Press Release, *FTC Adds Edward W. Felten as its Chief Technologist* (Nov. 4, 2010), *available at* www.ftc.gov/opa/2010/11/cted.shtm.

devices spanning various platforms and carriers, along with the software and other equipment needed to collect and preserve evidence.

Additionally, the FTC's Bureau of Consumer Protection assembled a team focusing on mobile technology. This group is conducting research, monitoring the various platforms, app stores, and applications, and training other FTC staff on mobile issues. In addition, in all of the FTC's consumer protection investigations, staff is examining whether the targets of investigations are using mobile technology in their operations.

C. Applying the FTC Act to the Mobile Arena

Although the FTC does not enforce any special laws applicable to mobile marketing, the FTC's core consumer protection law – Section 5 of the FTC Act – prohibits unfair or deceptive practices in the mobile arena.[13] This law applies to commerce in all media, whether traditional print, telephone, television, desktop computer, or mobile device. The Commission has several recent law enforcement and policy initiatives in the mobile arena, which build on the Commission's extensive law enforcement experience in the Internet and privacy areas.

1. Endorsement Law and Advertising Substantiation

The FTC brought a case last August applying FTC advertising law principles to the mobile apps marketplace. The Commission charged Reverb Communications, Inc., a public relations agency hired to promote video games, with deceptively endorsing mobile gaming applications in the iTunes store.[14] The company allegedly posted positive reviews of gaming apps using account names that gave the impression the reviews had been submitted by

---

[13] 15 U.S.C. § 45(a).

[14] *Reverb Commc'ns, Inc.*, FTC Docket No. C-4310 (Nov. 22, 2010) (consent order), *available at* www.ftc.gov/opa/2010/08/reverb.shtm.

disinterested consumers when they were, in actuality, posted by Reverb employees. In addition, the Commission charged that Reverb failed to disclose that it often received a percentage of the sales of each game. The Commission charged that the disguised reviews were deceptive under Section 5, because knowing the connections between the reviewers and the game developers would have been material to consumers reviewing the iTunes posts in deciding whether or not to purchase the games. In settling the allegations, the company agreed to an order prohibiting it from publishing reviews of any products or services unless it discloses a material connection, when one exists, between the company and the product.

The *Reverb* settlement demonstrates that the FTC's well-settled truth-in-advertising principles apply to new forms of mobile marketing. The mobile marketplace may offer advertisers new opportunities, but as in the offline world, companies must be able to substantiate claims made about their products. Developers may not make misrepresentations or unsubstantiated claims about their mobile apps, whether those claims are in banner ads, on a mobile website, in an app, or in app store descriptions. FTC staff is working to identify other violations of these well-established principles in the mobile context

2. Unauthorized Charges and Other Deceptive Conduct

FTC staff has active investigations into other unfair or deceptive conduct in the mobile arena. For example, staff is examining both the cramming of charges on consumers wireless phone bills and alleged inadequate disclosures of charges for in-app purchases.

Cramming is the practice of placing unauthorized charges on consumers' telephone bills. The FTC has aggressively prosecuted cramming violations in connection with landline telephone

bills for many years.[15] Mobile telephone accounts can also be used as a billing mechanism. On May 11, the FTC hosted a workshop on Phone Bill Cramming. The workshop examined how the mobile and landline billing platforms work, best practices for industry, and the development of cramming prevention mechanisms.[16]

Concerns about charges for in-app purchases in games and other apps that initially appear to be free is another issue of concern. Several members of Congress and others have raised concerns about purportedly free mobile apps directed to children that subsequently result in charges for products and services found within the applications, without adequate disclosures.[17] FTC staff is examining industry practices related to this issue.

3. Unsolicited Commercial Text Messages

Through enforcement of the CAN-SPAM Act[18], the Commission has long sought to protect consumers from unsolicited commercial email. Indeed, CAN-SPAM applies to email regardless of what type of computer or device is used to view and send the commercial email messages. Unsolicited text messages present problems similar to those addressed by CAN-

---

[15] *See, e.g., FTC v. INC21.com*, No. C 10-00022 WHA (N.D. Cal.) (summary judgment entered Sept. 21, 2010), *available at* www.ftc.gov/opa/2010/09/inc21.shtm; *FTC v. Nationwide Connections, Inc.*, No. Cv 06-80180 (S.D. Fla.) (final stipulated orders entered Apr. 11, 2008), *available at* www.ftc.gov/opa/2008/04/cram.shtm.

[16] *See* FTC Workshop, *Phone Bill Cramming*, *available at* www.ftc.gov/bcp/workshops/cramming/.

[17] Cecelia Kang, *Lawmakers Urge FTC to Investigate Free Kids Games on iPhone,* Washington Post (Feb. 8, 2011), *available at* www.washingtonpost.com/wp-dyn/content/article/2011/02/08/AR2011020805721.html.

[18] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701-7713.

SPAM, but unsolicited text messages present additional problems for mobile phone users.

In February, the Commission filed its first law enforcement action against a sender of unsolicited text messages and obtained a temporary restraining order suspending the defendant's challenged operations. The FTC alleged that Philip Flora sent more than 5 million unsolicited text messages – almost a million a week – to the mobile phones of U.S. consumers and that this was an unfair practice under Section 5 of the FTC Act.[19] Many consumers who received Flora's text messages – which typically advertised questionable mortgage loan modification or debt relief services – had to pay a fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans, thereby causing some consumers to incur additional charges on their monthly bill.[20]

4. Debt Collection Technology

The impact of mobile technology is also evident in the debt collection industry. On April 28, the Commission hosted a forum that examined the impact of new technologies on debt

---

[19] *FTC v. Flora*, CV11-00299 (C.D. Cal.) (Compl. filed Feb. 22, 2011), *available at* www.ftc.gov/opa/2011/02/loan.shtm. The complaint also alleges that Flora sent over the Internet unsolicited commercial email messages advertising his texting services. The emails did not include a valid opt-out mechanism and failed to include a physical postal address, in violation of the CAN-SPAM Act. In these emails, Flora offered to send 100,000 text messages for only $300. Further, the complaint charged that Flora deceptively claimed an affiliation with the federal government in connection with the loan modification service advertised in the text messages.

[20] While the financial injury suffered by any consumer may have been small, the aggregate injury was likely quite large. And, even for those consumers with unlimited messaging plans, Flora's unsolicited messages were harassing and annoying, coming at all hours of the day.

collection practices, including the technologies used to locate, identify, and contact debtors.[21] Panelists discussed the consumer concerns that arise when collectors contact debtors on their mobile phones, and whether some appropriate consumer consent should be required before a collector calls or sends text messages to a consumer's mobile phone. Commission staff is considering and analyzing the information received from the workshop and is preparing a summary report.

5. Mobile Payments

The use of mobile phones as a payment device also presents potential consumer protection issues.[22] As mentioned above, consumers can already charge goods and services, real or virtual, to their mobile telephone bills and app store accounts. Many other payment mechanisms and models are still developing, such as contactless payments systems that allow consumers to pay for products and services with the swipe of their smart phone.[23] Many, but not all, mobile payment systems are tied to traditional payment mechanisms such as credit cards. Staff is monitoring this emerging area for potential unfair or deceptive practices.

---

[21] FTC Workshop, *Debt Collection 2.0: Protecting Consumers As Technologies Change*, *available at* www.ftc.gov/bcp/workshops/debtcollectiontech/index.shtml.

[22] *See* Elizabeth Eraker, Colin Hector & Chris Hoofnagle, *Mobile Payment: The Challenge of Protecting Consumers and Innovation,* BNA, 10 Privacy & Security Law Report 212 (Feb. 7, 2011).

[23] *See* Darin Contini, Marianne Crowe, Cynthia Merritt, Richard Oliver & Steve Mott, Retail Payments Risk Forum, *Mobile Payments in the United States: Mapping Out the Road Ahead*, (Mar. 25, 2011), *available at* www.frbatlanta.org/documents/rprf/rprf_pubs/110325_wp.pdf; Smart Card Alliance, *Contactless Payment Growth and Evolution to Mobile NFC Payment are Highlights as Smart Card Alliance/CTST Conference Opens* (May 14, 2008), *available at* www.smartcardalliance.org/articles/2008/05/14/contactless-payment-growth-and-evolution-to-mobile-nfc-payment-are-highlights-as-smart-card-alliance-ctst-conference-opens.

III. Privacy Issues in the Mobile Arena

The rapid growth of new mobile services has provided enormous benefits to both businesses and consumers. At the same time, it has facilitated unprecedented levels of data collection, which are often invisible to consumers.

The Commission recognizes that mobile technology presents unique and heightened privacy and security concerns. In the complicated mobile ecosystem, a single mobile device can facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, app developers, analytics companies, and advertisers. And, unlike other types of technology, mobile devices are typically personal to the user, almost always carried by the user and switched-on.[24] From capturing consumers' precise location to their interactions with email, social networks, and apps, companies can use a mobile device to collect data over time and "reveal[] the habits and patterns that mark the distinction between a day in the life and a way of life."[25] Further, the rush of on-the-go use, coupled with the small screens of most mobile devices, makes it especially unlikely that consumers will read detailed privacy disclosures.

In recent months, news reports have highlighted the virtually ubiquitous data collection

---

[24] *See, e.g.*, Amanda Lenhart, Pew Internet & American Life Project, *Adults, Cell Phones and Texting* (Sept. 2, 2010), at 10, *available at* www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults/Overview.aspx ("65% of adults with cell phones say they have ever slept with their cell phone on or right next to their bed"); Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), at 73, *available at* www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones/Chapter-3/Sleeping-with-the-phone-on-or-near-the-bed.aspx (86% of cell-owning teens ages 14 and older have slept with their phones next to them).

[25] *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

by smartphones and their apps. Researchers have reported that both major smartphone platform providers collect precise location information from phones running their operating systems to support their device location services.[26] The *Wall Street Journal* has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique identifiers associated with a particular mobile device – that can be used to track and predict consumers' every move.[27] Not surprising, recent surveys indicate that consumers are concerned. For example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[28] The Commission has addressed these issues through a combination of law enforcement and policy initiatives, as discussed below.

A. Mobile Privacy: Enforcement Actions

The FTC's privacy cases have challenged companies that fail to protect the privacy and security of consumer information, including information obtained through mobile

---

[26] *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, Wall St. J. (Apr. 22, 2011), *available at* online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[27] *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, Wall St. J. (Apr. 23, 2011), *available at* online.wsj.com/article/SB10001424052748704547604576263 261679848814.html (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, Wall St. J. (Dec. 18, 2010), *available at* online.wsj.com/article/SB1000142405 274870436800457602775186703973O.html (documenting the data collection that occurs through many popular smartphone apps).

[28] NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location* (Apr. 21, 2011), *available at* blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location; *see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* (Mar. 2011), at 7, *available at* aa-download.avg.com/filedir/other/ Smartphone.pdf (64% of consumers worry about being tracked when using their smartphones).

communications. Two recent cases highlight the application of the FTC's privacy enforcement to the mobile marketplace.

First, the Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate a new social network, Google Buzz.[29] The Commission charged that Gmail users' associations with their frequent email contacts became public without the users' consent. As part of the Commission's proposed settlement order, Google must protect the privacy of all of its customers – including mobile users. For example, the order requires Google to implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.

Second, in the Commission's case against social networking service Twitter, the FTC alleged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.[30] As a result, hackers had access to private "tweets" and non-public user information – including users' mobile phone numbers – and took over user accounts, among them, those of then-President-elect Obama and Rupert Murdoch. The Commission's order, which applies to Twitter's collection and use of consumer data, including through mobile devices or apps, prohibits future misrepresentations and requires Twitter to maintain reasonable security and obtain independent audits of its security practices.

FTC staff has a number of additional active investigations regarding privacy issues

---

[29] *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment), *available at* www.ftc.gov/opa/2011/03/google.shtm.

[30] *Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* www.ftc.gov/opa/2011/03/twitter.shtm.

associated with mobile devices, including children's privacy.

B. Mobile Privacy: Policy Initiatives

In late 2009 and early 2010, the Commission held three roundtables to examine how changes in the marketplace have affected consumer privacy and whether current privacy laws and frameworks have kept pace with these changes.[31] At one roundtable, a panel focused on the privacy implications of mobile technology. Participants addressed the complexity of data collection through mobile devices; the extent and nature of the data collection, particularly with respect to location data; and the adequacy of privacy disclosures on mobile devices.[32] Based on the information received through the roundtables, FTC staff drafted a preliminary report ("Staff Report") proposing a new privacy framework consisting of three main recommendations, each of which applies to mobile technology.[33]

First, FTC staff recommended that companies adopt a "privacy by design" approach by building privacy protections into their everyday business practices, such as not collecting or retaining more data than they need to provide a requested service or transaction. Thus, for example, if an app provides only traffic and weather information to a consumer, it does not need

---

[31] *See* FTC, *Exploring Privacy: A Roundtable Series*, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[32] Transcript of Roundtable Record, *Exploring Privacy: A Roundtable Series* (Jan. 28, 2010) (Panel 4, "Privacy Implication of Mobile Computing"), at 238, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf.

[33] *See* FTC Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners William E. Kovacic and J. Thomas Rosch issued concurring statements available at http://ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively.

to collect call logs or contact lists from the consumer's device.

Second, staff recommended that companies provide simpler and more streamlined privacy choices to consumers. This means that all companies involved in data collection and sharing through mobile devices – carriers, handset manufacturers, operating system providers, app developers, and advertisers – should work together to provide such choices and to ensure that they are understandable and accessible on the small screen. The Staff Report also stated that companies should obtain affirmative express consent before collecting or sharing sensitive information, such as precise location data.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including streamlining their privacy disclosures to consumers.

After releasing the Staff Report, staff received 452 public comments on its proposed framework, a number of which implicate mobile privacy issues specifically. FTC staff is analyzing the comments and will take them into consideration in preparing a final report for release later this year.

C. Web Browsing and Do Not Track on Mobile Devices

The Staff Report included a recommendation to implement a universal choice mechanism for online tracking, including for purposes of delivering behavioral advertising, often referred to as "Do Not Track," and a majority of the Commission has expressed support for such a mechanism.[34] Behavioral advertising helps support online content and services, and many

---

[34] *See* FTC Staff Report, *supra* note 33; *see also Do Not Track: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. (Dec. 2, 2010), *available at* www.ftc.gov/os/testimony/101202donottrack.pdf (statement of the FTC, Commissioner Kovacic

consumers may value the personalization that it offers. However, the third-party tracking that underlies much of this advertising is largely invisible to consumers, some of whom may prefer not to have their personal browsing and searching information collected by companies with which they do not have a relationship.

The FTC repeatedly has called on stakeholders to develop and implement better tools to allow consumers to control the collection and use of their online browsing data,[35] and industry and other stakeholders have responded. In recent months a number of browser vendors – including Microsoft, Mozilla, and Apple – have announced that the latest versions of their browsers include, or will include, the ability for consumers to tell websites not to track their online activities.[36] Additionally, last month the World Wide Web Consortium[37] held a two-day

---

dissenting). Commissioner Kovacic believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. *See* FTC Staff Report, App. D. Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. *See id.*, App. E. To clarify, Commissioner Rosch continues to believe that a variety of questions need to be answered prior to the endorsement of any particular Do Not Track mechanism, including the consequences of the mechanism for consumers and competition.

[35] *See, e.g.*, *The State of Online Consumer Privacy, Hearing Before the S. Comm. on Commerce, Science & Transportatio*n, 112th Cong. (Mar. 16, 2011), *available at* www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf (statement of the FTC, Commissioner Kovacic dissenting); *Do Not Track: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce,* 111th Cong. (Dec. 2, 2010), *available at* www.ftc.gov/os/testimony/101202donottrack.pdf (statement of the FTC, Commissioner Kovacic dissenting); *see also FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[36] *See* Press Release, *Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9* (Dec. 7, 2010), *available at* www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx; Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities*, blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabiliti

workshop at which participants including academics, industry representatives, and privacy advocates discussed how to develop standards for incorporating "Do Not Track" preferences into Internet browsing.[38] The online advertising industry has also made important progress in this area. For example, the Digital Advertising Alliance, an industry coalition of media and marketing associations, is launching an enhanced notice program that includes an icon embedded in behaviorally targeted ads.[39] When consumers click on the icon, they can see more information about how the ad was targeted and delivered to them and are given the opportunity to opt out of receiving such ads, although collection of browsing information could continue.

These recent industry efforts to improve consumer control are promising, but they are still in the early stage and their effectiveness remains to be seen. As industry continues to explore technical options and implement self-regulatory programs and Congress continues to

---

es/ (Feb. 8, 2011); Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, Wall St. J. (Apr. 14, 2011), *available at* online.wsj.com/article/SB10001424052748703551304576261272308358858.html.

[37] The World Wide Web Consortium (W3C) is an international community whose "mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See* www.w3.org/Consortium/mission.html.

[38] *See* www.w3.org/2011/track-privacy/. This event followed a joint proposal by Stanford Law School's Center for Internet and Society and Mozilla for a header-based Do Not Track mechanism submitted to the Internet Engineering Task Force. *See* Do Not Track: A Universal Third-Party Web Tracking Opt Out (Mar. 7, 2011), *available at* tools.ietf.org/html/draft-mayer-do-not-track-00; *see also Mozilla Makes Joint Submission to IETF on DNT*, *available at* firstpersoncookie.wordpress.com/2011/03/09/mozilla-makes-joint-submission-to-ietf-on-dnt/.

[39] *See* Interactive Advertising Bureau Press Release, *Major Marketing Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising* (Oct. 4, 2010), *available at* www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

examine Do Not Track, five critical principles should be considered to make any Do Not Track mechanism robust and effective. Do Not Track should (1) be universal; (2) be easy to find and use; (3) be enforceable; (4) ensure that consumer choices are persistent; and (5) not only allow consumers to opt out of receiving targeted advertising, but also allow them to opt out of collection of behavioral data for all purposes that are not commonly accepted.[40]

The Staff Report asked whether Do Not Track should apply in the mobile context. At least for purposes of web browsing, the issues surrounding implementation of Do Not Track are the same on mobile devices and desktop computers. On both types of devices, the user could assert a Do Not Track choice, the browser would remember this choice, and the browser would send the Do Not Track request to other web sites visited. The technology underlying mobile apps, however, differs in some respects from web browsing (apps run outside of the browser, unlike web sites), and thus the Staff Report has asked for comment about the application of Do Not Track to mobile apps, and FTC staff is currently examining the technology involved in a Do Not Track mechanism for mobile apps.

Chairman Rockefeller has introduced Do Not Track legislation that would address desktop and mobile services.[41] The Commission supports the fundamental goals of this legislation – to provide transparency and consumer choice regarding tracking. Although the Commission has not taken a position on whether there should be legislation in this area, the Commission supports the approach in the proposed legislation, which would consider a variety

---

[40] For more detail concerning these five principles, see *The State of Online Consumer Privacy, Hearing Before the S. Comm. on Commerce, Science & Transportation*, *supra* note 35, at 16-17.

[41] Do Not Track Online Act of 2011, S. 913, 112th Cong. (2011).

of factors in implementing a Do Not Track mechanism, including the scope of the Do Not Track standard, the technical feasibility and costs, and how the collection of anonymous data would be treated under the standard. Indeed, the Commission agrees that any legislative mandate must give careful consideration to these issues, along with any competitive implications, as part of the Do Not Track rulemaking process. We would be pleased to work with Chairman Rockefeller, the Committee and Committee staff as they consider these important issues.

D. Children's and Teens' Mobile Privacy

The Commission has a long history of working to protect the privacy of young people in the online environment. In recent years, the advent of new technologies and new ways to collect data, including through mobile devices, has heightened concerns about the protection of young people when online.

1. Children's and Teen's Use of Mobile Technology

Children's and teens' use of mobile devices is increasing rapidly – in 2004, 45 percent of 12 to 17 year-olds had a cell phone; by 2009, that figure jumped to 75 percent.[42] Many young people are using their phones not just for calling or sending text messages, but increasingly for sending emails, web browsing, and using a host of apps that enable them to access social networks and make online purchases.[43] They are also using relatively new mobile apps that raise privacy concerns such as location-based tracking.[44] Even very young children have embraced

---

[42] Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), at 2, *available at* www.pewinternet.org/~/media//Files/Reports/2010/PIP-Teens-and-Mobile-2010.pdf.

[43] *Id.*

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

these new technologies. In one study, two-thirds of the children ages 4-7 stated they had used an iPhone, often one owned by a family member and handed back to them while riding in an automobile.[45]

2. Enforcement of the Children's Online Privacy Protection Rule

The Commission actively engages in law enforcement, consumer and business education, and rulemaking initiatives to ensure knowledge of, and adherence to, the Children's Online Privacy Protection Rule ("COPPA Rule"), issued pursuant to the Children's Online Privacy Protection Act of 1998.[46] The COPPA Rule requires operators of interactive websites and online services directed to children under the age of 13 , as well as operators of general audience sites and services having knowledge that they have collected information from children, to provide certain protections. In the past ten years, the Commission has brought 16 law enforcement actions alleging COPPA violations and has collected more than $6.2 million in civil penalties.

Just last week, the Commission announced its largest civil penalty in a COPPA action, a $3 million settlement against Playdom, Inc. The Commission alleged that the company, a leading developer of online multi-player games, as well as one of its executives, violated COPPA by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' prior consent.[47] While the allegations against

---

[45] Cynthia Chiong & Carly Shuler, Joan Ganz Cooney Center, *Learning: Is there an App for that?* (Nov. 2010), at 15, *available at* www.joanganzcooneycenter.org/upload_kits/learningapps_final_110410.pdf.

[46] The Commission's COPPA Rule is found at 16 C.F.R. Part 312. The COPPA statute is found at 15 U.S.C. § 6501 *et seq.*

[47] *United States v. Playdom, Inc.*, No. SACV11-00724 (C.D. Cal.) (final stipulated order filed May 11, 2011), *available at* www.ftc.gov/opa/2011/05/playdom.shtm.

Playdom do not specifically include the collection of information via mobile communications, the order, like all previous COPPA orders, applies to future information collected from children, whether it is collected via a desktop computer or a mobile computing device.

3. Review of the COPPA Rule

In April 2010, the Commission accelerated its review of the COPPA Rule, asking for comment on whether technological changes in the online environment warrant any changes to the Rule or to the statute.[48] In June 2010, the Commission also held a public roundtable to discuss the implications for COPPA enforcement raised by new technologies, including the rapid expansion of mobile communications.[49]

While the Rule review is ongoing, public comments and roundtable remarks reveal widespread consensus that the COPPA statute and the Rule were written broadly enough to encompass most forms of mobile communications without the need for statutory change.[50] For example, current technologies such as mobile applications, interactive games, voice-over-Internet services, and social networking services that access the Internet or a wide-area network

---

[48] *See* 75 Fed. Reg. 17,089 (Apr. 5, 2010). Although, of course, the Commission does not have the authority to amend the statute, it could recommend changes to Congress if warranted. Commission staff anticipates that proposed changes to the COPPA Rule, if any, will be announced in the next few months.

[49] Information about the June 2, 2010 COPPA Roundtable is located at http://www.ftc.gov/bcp/workshops/coppa/index.shtml. The public comments submitted in connection with the COPPA Rule review are available at http://www.ftc.gov/os/comments/copparulerev2010/index.shtm.

[50] *See, e.g.*, Comment of Center for Democracy and Technology (July 1, 2010), at 2, *available at* http://www.ftc.gov/os/comments/copparulerev2010/547597-00049-54858.pdf; Transcript of Roundtable Record, *COPPA Rule Review Roundtables* (June 2, 2010), at 14, (remarks of Ed Felten, Center for Information Technology Policy), *available at* http://www.ftc.gov/bcp/workshops/coppa/ COPPARuleReview_Transcript.pdf (hereinafter "COPPA Transcript").

are "online services" covered by COPPA.[51] There was less consensus as to whether certain mobile communications such as text messages are "online services" covered by COPPA. Certain commenters indicated that, depending on the details of the texting program – and provided that personal information is collected – COPPA could cover such programs.[52] Other commenters maintained that text messages cross wireless service providers' networks and short message service centers, not the public Internet, and that therefore such services are not Internet-based and are not "online services."[53] Commission staff is assessing new technologies to determine whether they are encompassed by, and conducted in accordance with, COPPA's parameters.

4. Consumer Education Initiatives for Children and Teens

The FTC has launched a number of education initiatives designed to encourage consumers of all ages to use technology safely and responsibly. In particular, the Commission's

---

[51] The statute's definition of "Internet," covering the "myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/ Internet Protocol," is plainly device neutral. 15 U.S.C. § 6502(6). In addition, the statutory use of the terms "website located on the Internet" and "online service," although undefined, is broadly understood to cover content that users can access through a browser on an ordinary computer or a mobile device, and services available over the Internet or that connect to the Internet or a wide-area network. *See* Comment of AT&T, Inc. (July 12, 2010), at 5, *available at* www.ftc.gov/os/comments/copparulerev2010/547597-00074-54989.pdf; Comment of Spratt (Apr. 18, 2010), *available at* www.ftc.gov/os/comments/copparulerev2010/ 547597-00004.html; COPPA Transcript, *supra* note 50, at 15 (remarks of Ed Felten).

[52] *See* COPPA Transcript, *supra* note 50, at 27-28 (remarks of Ed Felten).

[53] *See* Comment of CTIA (June 30, 2010), at 2-5, *available at* www.ftc.gov/os/comments/copparulerev2010/547597-00039-54849.pdf (citing the Federal Communications Commission's rules and regulations implementing the CAN-SPAM Act of 2003 and the Telephone Consumer Protection Act of 1991, finding that phone-to-phone SMS is not captured by Section 14 of CAN-SPAM because such messages do not have references to Internet domains).

educational booklet, *Net Cetera: Chatting with Kids About Being Online*,[54] 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. The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera*, and the agency has distributed more than 7.8 million print copies of the guide since it was introduced in October 2009. FTC staff are currently developing additional consumer education materials focused on mobile issues.

IV. CONCLUSION

The Commission is committed to protecting consumers, including children and teens, from unfair and deceptive acts in the burgeoning mobile marketplace. This dedication is reflected in the Commission's recent law enforcement actions and ongoing investigations, policy initiatives, and investment of resources to augment its mobile technical expertise and investigative tools. Protecting the privacy and security of consumer information is a critical component of the Commission's focus on mobile technologies and services. We will continue to bring law enforcement actions where appropriate and work with industry and consumer groups to develop workable solutions that allow companies to continue to innovate and give consumers the new products and services they desire.

---

[54] *Net Cetera* is available online at www.onguardonline.gov/pdf/tec04.pdf.